Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel.law
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444
Fax: 310-854-0812

Barry. R. Eichen [Admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [Admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
Ashley A. Smith [Admitted *Pro Hac Vice*]
asmith@njadvocates.com
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

Stephen M. Gorny [Admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [Admitted *Pro Hac Vice*]
chris@gornylawfirm.com
THE GORNY LAW FIRM, LC
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

Jay Barnes [Admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [Admitted *Pro Hac Vice*]
rod.chapel@gmail.com
BARNES & ASSOCIATES
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WINSTON SMITH; JANE DOE I; and JANE DOE II, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.; AMERICAN CANCER SOCIETY, INC.; AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.; MELANOMA RESEARCH FOUNDATION; ADVENTIST HEALTH SYSTEM; BJC HEALTHCARE; CLEVELAND CLINIC; and UNIVERSITY OF TEXAS - MD ANDERSON CANCER CENTER,

Defendants.

CASE NO. 5:16-cv-01282-EJD

DECLARATION OF JASON "JAY" BARNES

Date: April 13, 2017
Time: 9:00 a.m.
Crtrm.: 4, 5th Floor
Judge: Hon. Edward J. Davila

DECLARATION OF JASON "JAY" BARNES

I, Jason "Jay" Barnes, hereby declare as follows:

1. I am an attorney duly admitted to practice *pro hac vice* before this Court. I am a partner in the firm of Barnes & Associates, one of the law firms representing Plaintiffs Winston Smith, Jane Doe I, and Jane Doe II and the putative class in this action.

2. I submit this Declaration in support of Plaintiffs' Motion for Injunctive Relief. I make this Declaration based on my personal knowledge and if called as a witness I could and would competently testify to the matters stated herein.

3. So as to avoid confusion, the health care Defendant privacy policies attached as exhibits to this Declaration use the same letter designation used for the exhibits attached to the Complaint. Accordingly, while sequential, the exhibits attached to this Declaration are labeled F – L as were those attached to the Complaint and in each instance the same exhibit letter applies to each health care Defendant. Therefore, Exhibit F, both here and in the Complaint, refers to Defendant American Cancer Society ("ACS"), Exhibit G, both here and in the Complaint, refers to Defendant American Society of Clinical Oncology ("ASCO"), etc.

4. On August 21, 2015, I visited the website Cancer.org, which is run by ACS, and saved as a PDF the Privacy Policy posted on that website. A true and correct copy of said policy was attached to the Complaint as Exhibit F, and a true and correct copy is attached hereto as Exhibit F-1. On September 12, 2016, I again visited Cancer.org and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy is attached hereto as Exhibit F-2.

5. On December 29, 2015, I visited the website Cancer.net, which is run by ASCO, and saved as a PDF the Privacy Policy posted on that website. A true and correct copy of said policy was attached to the Complaint as Exhibit G, and a true and correct copy is attached hereto as Exhibit G-1. On September 12, 2016, I again visited Cancer.net and saved as a PDF the privacy policy posted on the website. A true and correct copy of said policy is attached hereto as Exhibit G-2.

6. On December 29, 2015, I visited the website Melanoma.org, which is run by

Defendant Melanoma Research Foundation, and saved as a PDF the Privacy Policy posted on that website. A true and correct copy of said policy was attached to the Complaint as Exhibit H, and a true and correct copy is attached hereto as Exhibit H-1. On September 12, 2016, I again visited Melanoma.org and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy is attached hereto as Exhibit H-2.

7. On December 29, 2015, I visited the website ShawneeMission.org, which is run by Defendant Adventist Health System for its hospital in Shawnee Mission, Kansas known as Shawnee Mission Hospital, and saved as a PDF the Privacy Policy posted on that website. A true and correct copy of said policy was attached to the Complaint as Exhibit I, and a true and correct copy is attached hereto as Exhibit I-1. On September 12, 2016, I again visited ShawneeMission.org and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy is attached hereto as Exhibit I-2.

8. On December 29, 2015, I visited the website BarnesJewish.org, which is run by Defendant BJC Healthcare, and saved as a PDF the "Joint Notice of Privacy Practices" and "Terms of Use and Privacy Statement" posted on the website. True and correct copies of said policies were attached to the Complaint as Exhibit J, and true and correct copies are attached hereto as Exhibit J-1. On September 12, 2016, I again visited BarnesJewish.org and saved as a PDF the "Joint Notice of Privacy Practices" and "Terms of Use and Privacy Statement" posted on the website. True and correct copies of said policies are attached hereto as Exhibit J-2.

9. On December 29, 2015, I visited the website ClevelandClinic.org, which is run by Defendant Cleveland Clinic, and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy was attached to the Complaint as Exhibit K, and a true and correct copy is attached hereto as Exhibit K-1. On September 12, 2016, I again visited ClevelandClinic.org and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy is attached hereto as Exhibit K-2.

10. On December 29, 2015, I visited the website MDAnderson.org, which is run by Defendant MD Anderson, and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy was attached to the Complaint as Exhibit L, and a true and correct

copy is attached hereto as Exhibit L-1. On September 12, 2016, I again visited MDAnderson.org and saved as a PDF the Privacy Policy posted on the website. A true and correct copy of said policy is attached hereto as Exhibit L-2.

11. On September 19, 2016, I visited the website Facebook.com and saved as a PDF the Statement of Rights and Responsibilities / Terms of Service posted on the website. Facebook purports on the website that this document was last revised on January 30, 2015. A true and correct copy of the Statement of Rights and Responsibilities is attached hereto as Exhibit M.

12. On September 19, 2016, I visited the website Facebook.com and saved as a PDF a true and correct copy of the Data Policy posted on the website. Facebook purports on the website that this document was last revised on January 30, 2015. A true and correct copy of the complete Data Policy is attached hereto as Exhibit N.

13. For the Court's convenience, attached hereto as Exhibit O is a true and correct copy of Plaintiffs' Opposition to Defendants' Motion to Dismiss (ECF No. 105) filed in this matter and referenced in the instant Motion.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed October 7, 2016, at Jefferson City, Missouri.

Jason "Jay" Barnes

EXHIBIT F-1

Online and Mobile Privacy Policy

Our Commitment to Privacy

The American Cancer Society ("ACS") respects the privacy of every individual who uses ACS-owned websites, mobile applications and other online products and services (collectively, "Site"). This notice applies to our information collection practices for this Site. Because your privacy is important to us, we provide you with notice and choices about the collection and use of your information. To make this notice easy to find, links are provided at the bottom of our homepage and on every page within our www.cancer.org website. Additionally, each page that requests personally identifiable information reminds you of the importance of your privacy and provides a link to the privacy policy. By accessing this you accept the practices described in this Privacy Notice. You may click on any underlined word to receive a more in-depth explanation of the term.

Use of Cookies

We use cookies, small files that are sent to your Web browser and stored on your computer's hard drive, to improve

your digital experience. The cookie is used to speed up your access to the Site and the information you wish to see, but it does not contain any personal information. The majority of Web browsers accept cookies, but the "help" menu on your browser should give you options for preventing, accepting, or receiving notice of new cookies. However, please be aware that if you block cookies, some website functionality may be lost.

Data Collection

We collect two types of information:

Standard Web server traffic pattern information. General traffic, site usage, browser information and length of stay information is collected and stored in log files. This type of information is shared externally only on an aggregated basis.

Personal information. We do not collect personally identifiable information from you unless you provide it to us voluntarily and knowingly. If you personalize a Site, volunteer, order a book, request information, or donate, for example, we may collect the following information: first and last name, street address, city, state, zip code, telephone number, email address, and subject of inquiry.

Personal information may be needed for certain optional online activities:

Registration: If you choose to customize the Web site to your needs by becoming a registered www.cancer.org Web user, we retain the preferences you select so that you will not have to reenter the information each time you access our Web site. These preferences may include requests for email, news, information on specific cancer types, language preferences, and interest group selections (patient, medical professional, volunteer). You can access your profile by entering your user name and password each time you use the Web site. You are not required, however, to enter your name or mailing address.

If you register to participate in an ACS event, such as Relay For Life or Making Strides Against Breast Cancer, using our event registration site, we may ask you if you are a cancer survivor. This information is useful for event purposes. Further, if you elect to use our referral service to inform a friend about the event registration site, we will ask you for your friend's name and address. We will store this information in order to send your friend a one-time email inviting him or her to visit the site.

Book orders: If you choose to order a book, we collect standard credit card information (card number, card type, expiration date) and keep a record of your financial transaction. Credit card numbers are held only until the charge can be processed (usually several minutes), then the number is only available to Customer Service for purposes of problem resolution.

Contributions: If you choose to donate to our organization, we maintain a record of your contribution. Your financial information will be treated as described above in "Book orders."

Requests: If you submit an online request for ACS products such as free brochures, or submit a question through a "contact us" query, we may have to gather additional information from you to respond to your request. Such information will vary with the request but often includes name, shipping address, telephone number, and email address.

Public Forums: If you choose to participate in a chat room, discussion board, news group or another public forum that we make available to our users, please remember that any information that you disclose in these areas becomes public information. You should exercise caution when deciding whether or not to disclose your personal information.

Letter to Congress: If you choose to generate an email to your Congressional representative on our site, we receive a blind copy of the email. We may use your letter or information from your letter to further educate Members of Congress about our cancer advocacy priorities.

Data Use

We limit the use of information provided to us on our Site to the following:

Internal Use

If you do not make a service request, donation, purchase, or otherwise identify yourself, we will have no personally identifiable information about you. We will only use aggregate information derived, in part, from your use of our site to

improve our site and our service to you.

If you provide personal information, we may enter your name into our constituent database and contact you in order to:
Complete voluntary surveys seeking feedback for quality and service improvement purposes.
Supply you with information including cancer related health news, ACS programs, events and services.
Request voluntary time or monetary contributions to ACS.
Request your participation in an ACS research study.

We collect the email addresses of those who communicate with us by email. Inquiries may be forwarded to the appropriate ACS department for response and may be entered into our constituent database. If your name is entered into the database, we may contact you (see (2) above).

External Use

Your health-related information is privileged and confidential and will not be shared or released to any organization or business entity other than those affiliated with or working in conjunction with ACS as follows:

We use third parties to provide you with the following services:
Cancer Profiler: Disclosure of personal information is optional when using the cancer profiler. Additional services offered by NexCura are covered by their privacy policy and may require payment and disclosure.

Clinical Trials: If you are considering clinical trial participation and would like to use the American Cancer Society Clinical Trials Matching Service, you must register with www.cancer.org and complete a screening questionnaire. This service is offered through a partnership between the American Cancer Society and the Coalition of Cancer Cooperative Groups. As part of the matching process, the Society and the Coalition will share your information with each other. If requested, the Society will then contact you to discuss the details or provide further information.

We occasionally make our constituent names and postal addresses available to other reputable non-profit organizations. We have found this to be the most cost-effective method of increasing our database of potential constituents and hope that you value the information they send you. Your name is only available to these carefully screened organizations for a limited time and it is de-identified, such that it is not associated with the American Cancer Society. Other organizations will not have continued access to your name and address unless you choose to respond to their initial mailing. We do not share email addresses or health related data. Information gathered as part of Cancer Profiler or Clinical Trials (above) is not shared.

We occasionally hire other companies to provide limited services on our behalf. We will only provide those companies the information they need to deliver the service and prohibit them from using that information for any other purpose.

We have relationships with companies that conduct charitable sales promotions and commercial coventures that support us in our mission and activities. If you provide us with your mailing address, we may pass your contact information to these companies so that they may ask you if you are interested in receiving their services. Your choice to use their services will benefit us; the amount of money we receive from these entities as a result of your participation is disclosed at the time you are contacted about the service. You are under no obligation to respond and the companies are restricted from using your contact information for any other purpose. Information gathered as part of Cancer Profiler or Clinical Trials (above) is not shared.

Your Options

We respect your privacy and allow you to restrict internal and external sharing of your personal information. We recognize that you may wish to limit the ways in which we contact you and we offer the following options:

Do not contact me by telephone.
Do not contact me by postal mail.
Do not contact me by email.
Do not share my contact information with other non-profit organizations.
Do not contact me with fundraising requests supporting the American Cancer Society.
Limit your fundraising appeals to semiannual solicitations only.

Do not contact me or share my information with anyone.

For more information on how to inform us of any desired restrictions, please click on the following link: opt out. If you contact us with an opt-out request, all reasonable efforts will be taken to ensure that you will not receive any of the selected communications from us in the future. If you do not wish to opt out at this time, you may do so at a later date should you so desire.

If you opt back into a specific service, you will receive communication in that manner, regardless of your overall opt out selections. These services may include newsletter subscriptions or email communication by asking a question using "Contact Us."

Access

Upon request, we will provide you with the information we maintain about you so that you may request corrections. This information will be sent via postal mail, which we believe is the most secure method of communication. Please contact us by email at privacyrequest@cancer.org or in writing at:

Security and Privacy Requests
The American Cancer Society National Cancer Information Center
11701 Stonehollow Dr
Austin, TX 78758

To protect your privacy and security, we will take reasonable steps to verify your identity before providing information or making corrections.

Data Security

We are committed to protecting the security of your personal information and to honoring your choices for its intended use. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we strive to maintain physical, electronic, and administrative safeguards.

We process your financial transactions securely using the Payment Card Industry Data Security Standard ("PCI DSS") (the credit card industry's most stringent security standard). Examples of our security measures include: physical, electronic, and procedural safeguards; sophisticated security monitoring tools; documented security policies; use of strong encryption (e.g., SSL) for transmissions of Order Information to and from our credit card processor; restricted access of personally identifiable information; and, periodic security audits.

Inside ACS, data is stored in password-controlled servers. Our staff and volunteers are educated about the importance of safeguarding your information and we are committed to holding them accountable for protecting your confidentiality. However, such precautions do not guarantee Site is invulnerable to all security breaks. ACS makes no warranty, guarantee, or representation that the use of our Site is protected from viruses, security threats, or other vulnerabilities and that your information will always be secure.

Whenever ACS permits an external third party to access personally-identifiable information, appropriate procedures are followed to help ensure that the information is used only for authorized purposes and by authorized persons in a manner consistent with the choices ACS constituents have made under this statement, and that the security, integrity and privacy of the information is maintained. While ACS will employ procedures to help ensure that your information is only used for authorized purposes as described above, we cannot make any guarantees with respect to the actions or policies of such third parties.

Links Within Our Site

Internal Links

Because of the various programs and services at ACS, there are several privacy notices to inform our constituents of policies specific to the activity in which they are participating. Please click on any one of the following links to learn more:

Cancer Survivors Network

Continuing Medical Education: Online Database

External Links

Our privacy policies apply only to your use of an ACS Site. The www.cancer.org website contains links to other sites, including sites that have a special relationship with us. We do not disclose personably identifiable information to those operating linked sites and we are not responsible for their privacy practices. Links to other sites do not imply an endorsement of the materials or policies on those websites. You should read the privacy policies of each site you visit to determine what information that site may be collecting about you.

Contact Us

This privacy statement will be updated periodically and posted on our Site. It applies only to our on-line practices and does not encompass other areas of the organization. Please click on one of the links provided under Internal Links to read other ACS privacy statements. It applies to the on-line practices of ACS. References to "American Cancer Society", "ACS", "we", "us" and "our" are references to American Cancer Society, Inc. and its affiliates, staff and volunteers. We reserve the right to change this policy at any time by posting revisions. You agree to review the Privacy Policies each time you use our Site so that you are aware of any modifications. By accessing or using the Site, you agree to be bound by all of the terms and conditions of the ACS Online and Mobile Application Privacy Policy as posted at the time of your access or use. If you have any questions about our policy or our compliance, you may send us an email at privacyrequest@cancer.org or write to:

Security and Privacy Requests
The American Cancer Society National Cancer Information Center
11701 Stonehollow Dr
Austin, TX 78758

Policy Updates

We reserve the right to update this policy at any time. Any changes will be effective immediately upon the posting of the revised policy.

About Us Topics

- Who We Are
- How We Help You
- Honoring People Who Are Making A Difference
- Global Health
- ACS Policies
- Press Room
- Employment Opportunities
- Dr. Len's Blog
- Gift Shop

Cancer Facts & Statistics
Online Support Communities
Relay Recess
Employment
Global Health
News About Cancer
Donate a Car
Become a Supplier
Finish the Fight
Expert Voices Blog
Report Fraud or Abuse
Press Room
Mobile Site

Help | Site Map | Privacy | Accessibility | Terms of Use | State Fundraising Notices | Site Comments

Better Business Bureau
Health On The Net
National Health Council

EXHIBIT F-2

Online and Mobile Privacy Policy

Our Commitment to Privacy

The American Cancer Society (“ACS”) respects the privacy of every individual who uses ACS-owned websites, mobile applications and other online products and services (collectively, "Site"). This notice applies to our information collection practices for this Site. Because your privacy is important to us, we provide you with notice and choices about the collection and use of your information. To make this notice easy to find, links are provided at the bottom of our homepage and on every page within our **www.cancer.org** website. Additionally, each page that requests personally identifiable information reminds you of the importance of your privacy and provides a link to the privacy policy. By accessing this you accept the practices described in this Privacy Notice. You may click on any underlined word to receive a more in-depth explanation of the term.

Use of Cookies

We use cookies, small files that are sent to your Web browser and stored on your computer's hard drive, to improve your digital experience. The cookie is used to speed up your access to the Site and the information you wish to see, but it does not contain any personal information. The majority of Web browsers accept cookies, but the “help” menu on your browser should give you options for preventing, accepting, or receiving notice of new cookies. However, please be aware that if you block cookies, some website functionality may be lost.

Data Collection

We collect two types of information:

1. Standard Web server traffic pattern information. General traffic, site usage, browser information and length of stay information is collected and stored in **log files**. This type of information is shared externally only on an aggregated basis.

2. Personal information. We do not collect personally identifiable information from you unless you provide it to us voluntarily and knowingly. If you personalize a Site, volunteer, order a book, request information, or donate, for example, we may collect the following information: first and last name, street address, city, state, zip code, telephone number, email address, and subject of inquiry.

   Personal information may be needed for certain optional online activities:

   Registration: If you choose to customize the Web site to your needs by becoming a registered www.cancer.org Web user, we retain the preferences you select so that you will not have to reenter the information each time you access our Web site. These preferences may include requests for email, news, information on specific cancer types, language preferences, and interest group selections (patient, medical professional, volunteer). You can access your profile by entering your user name and password each time you use the Web site. You are not required, however, to enter your name or mailing address.

   If you register to participate in an ACS event, such as Relay For Life or Making Strides Against Breast Cancer, using our event registration site, we may ask you if you are a cancer survivor. This information is useful for event purposes. Further, if you elect to use our referral service to inform a friend about the event registration site, we will ask you for your friend’s name and address. We will store this information in order to send your friend a one-time email inviting him or her to visit the site.

   Book orders: If you choose to order a book, we collect standard credit card information (card number, card type, expiration date) and keep a record of your financial transaction. Credit card numbers are held only until the charge can be processed (usually several minutes), then the number is only available to Customer Service for purposes of

problem resolution.

Contributions: If you choose to donate to our organization, we maintain a record of your contribution. Your financial information will be treated as described above in “Book orders.”

Requests: If you submit an online request for ACS products such as free brochures, or submit a question through a “contact us” query, we may have to gather additional information from you to respond to your request. Such information will vary with the request but often includes name, shipping address, telephone number, and email address.

Public Forums: If you choose to participate in a chat room, discussion board, news group or another public forum that we make available to our users, please remember that any information that you disclose in these areas becomes public information. You should exercise caution when deciding whether or not to disclose your personal information.

Letter to Congress: If you choose to generate an email to your Congressional representative on our site, we receive a blind copy of the email. We may use your letter or information from your letter to further educate Members of Congress about our cancer advocacy priorities.

Data Use

We limit the use of information provided to us on our Site to the following:

Internal Use

1. If you do not make a service request, donation, purchase, or otherwise identify yourself, we will have no personally identifiable information about you. We will only use aggregate information derived, in part, from your use of our site to improve our site and our service to you.

2. If you provide personal information, we may enter your name into our constituent database and contact you in order to:
    - Complete voluntary surveys seeking feedback for quality and service improvement purposes.
    - Supply you with information including cancer related health news, ACS programs, events and services.
    - Request voluntary time or monetary contributions to ACS.
    - Request your participation in an ACS research study.

3. We collect the email addresses of those who communicate with us by email. Inquiries may be forwarded to the appropriate ACS department for response and may be entered into our constituent database. If your name is entered into the database, we may contact you (see (2) above).

External Use

Your health-related information is privileged and confidential and will not be shared or released to any organization or business entity other than those affiliated with or working in conjunction with ACS as follows:

1. We use third parties to provide you with the following services:
    a. Cancer Profiler: Disclosure of personal information is optional when using the **cancer profiler**. Additional services offered by **NexCura** are covered by their **privacy policy** and may require payment and disclosure.

    b. Clinical Trials: If you are considering **clinical trial participation** and would like to use the American Cancer Society Clinical Trials Matching Service, you must register with www.cancer.org and complete a screening questionnaire. This service is offered through a partnership between the American Cancer Society and the **Coalition of Cancer Cooperative Groups**. As part of the matching process, the Society and the Coalition will share your information with each other. If requested, the Society will then contact you to discuss the details or provide further information.

2. We occasionally make our constituent names and postal addresses available to other reputable non-profit organizations. We have found this to be the most cost-effective method of increasing our database of potential constituents and hope that you value the information they send you. Your name is only available to these carefully screened organizations for a limited time and it is de-identified, such that it is not associated with the American Cancer Society. Other organizations will not have continued access to your name and address unless you choose to respond to their initial mailing. We do not share email addresses or health related data. Information gathered as part of

Cancer Profiler or Clinical Trials (above) is not shared.

3. We occasionally hire other companies to provide limited services on our behalf. We will only provide those companies the information they need to deliver the service and prohibit them from using that information for any other purpose.

4. We have relationships with companies that conduct charitable sales promotions and commercial coventures that support us in our mission and activities. If you provide us with your mailing address, we may pass your contact information to these companies so that they may ask you if you are interested in receiving their services. Your choice to use their services will benefit us; the amount of money we receive from these entities as a result of your participation is disclosed at the time you are contacted about the service. You are under no obligation to respond and the companies are restricted from using your contact information for any other purpose. Information gathered as part of Cancer Profiler or Clinical Trials (above) is not shared.

Your Options

We respect your privacy and allow you to restrict internal and external sharing of your personal information. We recognize that you may wish to limit the ways in which we contact you and we offer the following options:

1. Do not contact me by telephone.
2. Do not contact me by postal mail.
3. Do not contact me by email.
4. Do not share my contact information with other non-profit organizations.
5. Do not contact me with fundraising requests supporting the American Cancer Society.
6. Limit your fundraising appeals to semiannual solicitations only.
7. Do not contact me or share my information with anyone.

For more information on how to inform us of any desired restrictions, please click on the following link: **opt out**. If you contact us with an opt-out request, all reasonable efforts will be taken to ensure that you will not receive any of the selected communications from us in the future. If you do not wish to opt out at this time, you may do so at a later date should you so desire.

If you opt back into a specific service, you will receive communication in that manner, regardless of your overall opt out selections. These services may include newsletter subscriptions or email communication by asking a question using “Contact Us.”

Access

Upon request, we will provide you with the information we maintain about you so that you may request corrections. This information will be sent via postal mail, which we believe is the most secure method of communication. Please contact us by email at **privacyrequest@cancer.org** or in writing at:

Security and Privacy Requests
The American Cancer Society National Cancer Information Center
11701 Stonehollow Dr
Austin, TX 78758

To protect your privacy and security, we will take reasonable steps to verify your identity before providing information or making corrections.

Data Security

We are committed to protecting the security of your personal information and to honoring your choices for its intended use. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we strive to maintain physical, electronic, and administrative safeguards.

We process your financial transactions securely using the Payment Card Industry Data Security Standard ("PCI DSS") (the credit card industry's most stringent security standard). Examples of our security measures include: physical, electronic, and procedural safeguards; sophisticated security monitoring tools; documented security policies; use of strong encryption (e.g., **SSL**) for transmissions of Order Information to and from our credit card processor; restricted access of personally identifiable information; and, periodic security audits.

Inside ACS, data is stored in password-controlled servers. Our staff and volunteers are educated about the importance of safeguarding your information and we are committed to holding them accountable for protecting your confidentiality. However, such precautions do not guarantee Site is invulnerable to all security breaks. ACS makes no warranty, guarantee,

or representation that the use of our Site is protected from viruses, security threats, or other vulnerabilities and that your information will always be secure.

Whenever ACS permits an external third party to access personally-identifiable information, appropriate procedures are followed to help ensure that the information is used only for authorized purposes and by authorized persons in a manner consistent with the choices ACS constituents have made under this statement, and that the security, integrity and privacy of the information is maintained. While ACS will employ procedures to help ensure that your information is only used for authorized purposes as described above, we cannot make any guarantees with respect to the actions or policies of such third parties.

Links Within Our Site

Internal Links

Because of the various programs and services at ACS, there are several privacy notices to inform our constituents of policies specific to the activity in which they are participating. Please click on any one of the following links to learn more:

- **Cancer Survivors Network**
- **Continuing Medical Education: Online Database**

External Links

Our privacy policies apply only to your use of an ACS Site. The **www.cancer.org** website contains links to other sites, including sites that have a special relationship with us. We do not disclose personably identifiable information to those operating linked sites and we are not responsible for their privacy practices. Links to other sites do not imply an endorsement of the materials or policies on those websites. You should read the privacy policies of each site you visit to determine what information that site may be collecting about you.

Contact Us

This privacy statement will be updated periodically and posted on our Site. It applies only to our on-line practices and does not encompass other areas of the organization. Please click on one of the links provided under Internal Links to read other ACS privacy statements. It applies to the on-line practices of ACS. References to "American Cancer Society", "ACS", "we", "us" and "our" are references to American Cancer Society, Inc. and its affiliates, staff and volunteers. We reserve the right to change this policy at any time by posting revisions. You agree to review the Privacy Policies each time you use our Site so that you are aware of any modifications. By accessing or using the Site, you agree to be bound by all of the terms and conditions of the ACS Online and Mobile Application Privacy Policy as posted at the time of your access or use. If you have any questions about our policy or our compliance, you may send us an email at **privacyrequest@cancer.org** or write to:

Security and Privacy Requests
The American Cancer Society National Cancer Information Center
11701 Stonehollow Dr
Austin, TX 78758

Policy Updates

We reserve the right to update this policy at any time. Any changes will be effective immediately upon the posting of the revised policy.

EXHIBIT G-1

Privacy Policy

Last updated December 31, 2011

Contents

1. Introduction

The **American Society of Clinical Oncology** (hereafter "**ASCO**," "**we**," or "**us**") respects your privacy and is committed to being transparent about how and when ASCO collects, uses, and safeguards the information we collect through our websites. We recognize that cancer is a personal disease, and we want you to feel as comfortable as possible visiting ASCO's websites and using our services. To fulfill our mission, ASCO must appropriately use information in order to better serve you. This Privacy Policy will tell you:

- who collects information,
- what information is collected and how this is done,
- how ASCO uses and discloses the information that is collected,
- your rights to view and correct information submitted voluntarily,
- your rights to opt-out, opt-in, or limit specific uses and disclosures of your information,
- what security procedures we use to protect your information,
- how the interactive areas of the Website operate,
- how we comply with the Children's Online Privacy Protection Act, and
- where you can get questions answered about this Privacy Policy.

We hope that reading this Privacy Policy gives you a clear idea of how we manage information about you. Throughout this Privacy Policy, we have underlined various terms and hot-linked them to our Glossary (Section 13 of this Privacy Policy), or hot-linked to a relevant Section within this Privacy Policy, to help you better understand their meaning.

2. Certain General Principles, Terms, and Disclaimers

This Privacy Policy applies to all personal information about you in the possession of ASCO, including information obtained through ASCO's websites: the ASCO website (www.asco.org), together with all other websites operated by ASCO, including without limitation the Cancer.Net website (www.cancer.net), the *Journal of Clinical Oncology* website (jco.ascopubs.org), the *Journal of Oncology Practice* website (jop.ascopubs.org), the Oncology Career Centerâ¢ website (www.careers.jco.org), the Quality Oncology Practice Initiative website (qopi.asco.org), the ASCO University website (university.asco.org), the CancerProgress.net website (www.cancerprogress.net) and the ASCO Connection website (connection.asco.org) (collectively, the "Website"). By using, accessing, or registering with the Website, you consent to our collection and use of your personal information in accordance with this Privacy Policy.

This Privacy Policy does not supersede the Terms and Condition of Use that governs your use of the Website. Any conflict between the two shall be determined in favor of the Terms and Conditions of Use. ASCO may change this Privacy Policy at any time and any changes will be effective immediately upon posting to the Website, so please check back regularly to ensure you read and understand our current privacy policies.

While information is critical to our ability to provide high quality service to you, our most important asset is the trust that our visitors place in how we provide that service. Keeping visitor information secure, and using it only as our visitors would want us to, is a top priority for all of us at ASCO. Consequently our privacy standards are designed to, on a commercially reasonable basis:

- collect and use only the minimum information necessary for us to deliver high quality service to users, to administer our business, and to let you know of

products and services that are available from ASCO and trusted third parties;
- protect the information our visitors share with us, maintaining strong standards of security and confidentiality;
- require any other organization that we retain or engage to provide support services to us to conform to our privacy standards; and
- keep visitor files, if any, complete, up to date, and accurate.

We do not collect Personally Identifiable Information from users browsing the Website. We do use first and third party Cookies to collect basic technological information about how visitors use the Website as described more fully in Section 4. This data is used to improve content, site performance, and services for our visitors.

Some features on the Website may require you to register as a user and to receive our authorization before you can use those particular features, including forums, mailing lists, meeting registrations, and other services. In order for you obtain our authorization to use those features and to be considered a registered user, you may be required to provide us with certain Personally Identifiable Information ("PII") about you or your business. The PII we collect can include names, addresses, e-mail addresses, telephone numbers, fax numbers, education and certifications, areas of specialty, credit card numbers, and other forms of PII.

Once we have authorized you as a registered user, we may provide you with a customer identification number and you will select a unique Username and Password. Generally, you will be able to change your Password and update any PII you have given us (instructions on how to make these changes can be found in Section 6 of this Privacy Policy).

If you have access to the Website as a designated representative of a business, ASCO may terminate your right to use the Website upon notification that you are no longer a designated representative for that business.

If you are submitting PII on behalf of others in your family, business or other organization for registration purposes or otherwise, you represent that you have their permission, agreement and full authorization to provide this information to us. We reserve the right (a) to ask you to provide evidence of your authority at any time during, or even after, the submission process and (b) to contact those individuals to confirm your authority at any time. If we determine that your authority has not been properly obtained, we may immediately and without notice to you discontinue your authorized use of those features of the Website for which you have registered.

3. Who Collects Information Through the Website

Subject to this Privacy Policy, the Terms and Conditions of Use, and any other rules or policies applicable to the Website, ASCO collects the information described in this policy through the Website.

In addition, ASCO has engaged third party vendors to help us manage our web presence and allow us to better serve our web visitors. Personal information submitted to ASCO through third party managed pages may be shared with these vendors as necessary for completing authorized transactions. These third-party managed pages include the *Journal of Clinical Oncology* website (jco.ascopubs.org), the *Journal of Oncology Practice* website (jop.ascopubs.org), the Oncology Career Centerâ¢ website (www.careers.jco.org), portions of the Career Opportunities at ASCO page (www.asco.org/about-asco/working-asco), and portions of ASCO in Action (ascoaction.asco.org).

ASCO has also provided external links to other websites in order to provide those who use the Website with a better, more fulfilling experience. Once you enter another website (whether through an advertisement, service or content link), be aware that ASCO is not responsible for the privacy practices of such other sites (see also Section 10 of the Terms and Conditions of Use). We encourage you to look for and review the privacy statements of each and every website that you visit through a link or sponsorship notice.

4. Information We Collect and How it is Used

If you use the Website without registering, we will only collect anonymous Non-Personal Information ("NPI"), about you through the use of first and third party Cookies and other technical means (described in more detail in this Section 4).

If you choose to register with the Website to use interactive or other specific services, we require you to submit certain PII, such as your name, address, e-mail address, telephone number, fax number, education and certification, areas of specialty, and credit card number. While you may use some of the functionality of the Website without registration, many specific tools and services on the Website require registration and your submission of PII.

How we collect NPI. We collect certain NPI about your use of the Website through our use of first and third party Cookies and through other technical means (e.g. Click Stream Information such as log files, Web Beacons, etc.). This NPI includes information about the date and time you visit the Website, which pages you view, how you arrive at the Website (through referring links or otherwise), how much time you spend on the Website, your IP address, and the type of Browser and operating system you use.

We encourage you to research online resources and learn about not only Cookies but also the other technical means through which information about you may be collected through websites you visit. Your Browser can be set to reject all Cookies. A "help" section of most Browsers' toolbar usually offers instructions on how to reset the browser to reject Cookies.

If you reject our Cookies, certain functions and conveniences of the Website may not

work properly, including those sections that are only available to registered users, but we believe you do not have to accept our Cookies in order to productively use the Website.

In addition, if you visit the Website through a link from an email newsletters sent by ASCO, our system will log such information as what links the you click through from the e-mail to the Website, the date and time of your click through, the name of the link or source from which the message was sent, the tracking URL number, and the destination page.

Anonymous nature of NPI; linking of NPI and PII. Generally, the NPI we collect about you is attached to arbitrary, anonymous system names that are assigned to visitors when they enter the Website. Please note, however, that during the registration process, or at other times during your use of the Website, we may ask for your permission to link your NPI with your PII. In addition, the providers of third party Cookies may have the ability to link your activities on the Website with your browsing activities elsewhere on the Internet.

Examples of how we may use NPI. The anonymous NPI we obtain from you is generally used to render, administer, and improve the Website, our services, and our business. We may use NPI to do any of the following (please note that this list is representative and provided only to assist you in understanding how we might use the NPI we collect).

- To help dynamically generate content on web pages or in newsletters.
- To statistically monitor how many people are using the Website.
- To track generic user behavior (see, for example, the definition of "Click Stream Information").
- To monitor how many people open our emails.
- To help us evaluate the purpose our users undertake certain activities, including those listed immediately above.
- To determine the popularity of certain content.
- To facilitate users' log-in and navigation and as session timers.
- To restrict underage use of our services.

Disclosure of Aggregate Information. ASCO may provide Aggregate Information to third parties. For example, we might inform third parties regarding the number of users of the Website and the activities they conduct while on the Website. We might for example inform a pharmaceutical company (that may or may not be sponsor of the Website) that "30% of our users live east of the Mississippi" or that "25% of our users have tried alternative medicine." We require parties with whom we share Aggregate Information to agree that they will not attempt to make this information PII, such as by combining it with other databases.

How we collect PII. The PII that we collect and store generally consists of information gathered when you register with the Website for specific services and/or when you

update any registration or profile information, but may also include other data input, forms, and information you provide to us whether electronically, by phone, by fax, in writing, in person, or by any other means. Your PII may also include information about your transactions and experiences with ASCO, including account balances and purchasing activity. If you provide us with PII through the Website, we will give you the opportunity to "Opt-Out" of receiving future communications from us related to the specific service for which we requested that information. Section 7 of this Privacy Policy more specifically describes how to manage your communications preferences and to opt-in or opt-out of communications from us.

How we use PII. We use PII, and any data, personal or otherwise, that you provide and which may be saved on the Website, to provide our products and services. In addition to the ways in which we may use NPI, examples of the ways in which we may use PII include but are not limited to:

- To respond to your questions.
- To provide to you the services or subscriptions you select.
- To contact you regarding ASCO events or other news.
- To send you information you request.
- To send and manage surveys.
- To advise you of products or services that may be available through ASCO.
- To notify you about website maintenance, updates, and new features.
- To contact you as needed to address a suspected violation of the Terms and Conditions of Use, this Privacy Policy, or any other rules or policies applicable to the Website.
- To inform you of significant changes to this Privacy Policy.
- To manage membership and volunteer functions.
- To confirm or fulfill purchase and registration requests.
- To display content we think may be of interest to you and otherwise help us customize what you see when you visit the Website.
- To solicit user feedback to assess user-satisfaction or other needs and interests.
- To help us in creating new tools, features, and services.
- To send you materials on behalf of trusted third parties.
- Otherwise in rendering, administering, and improving the Website, our services, and our business.

ASCO only discloses your PII to third parties under those circumstances outlined in Section 5.

If you are registered to use particular services, you acknowledge and also consent to our tracking activities and use of the Website under your username in connection with those services (e.g., in order to confirm and fill orders, maintain quality control and contact you concerning your orders, transactions, or subscriptions, should it be necessary or appropriate to do so).

E-Commerce Transactions. When you place an order online with us, register for a

conference, or pay your dues electronically, your personal information and credit card information are encrypted using industry-standard SSL Encryption technology before being sent over the Internet. We submit to the appropriate credit card clearinghouse only the information necessary to collect payment. All credit card information retained by ASCO, including credit card numbers if you elect to store them on your account, is compliant with Payment Card Industry data security standards.

Our (a) use of your PII and (b) handling of any e-mail sent to us by you through the Website (with regard to communications from clients and the public), will in each case be in a manner consistent with the Terms and Conditions of Use, this Privacy Policy, any other rules or policies applicable to this Website, and all applicable laws, rules, and regulations.

5. Disclosure of Your Personally Identifiable Information

ASCO will only disclose your PII to third parties under the following circumstances:

- disclosure to corporate affiliates of ASCO, including the Conquer Cancer Foundation (www.conquercancerfoundation.org) and the Institute for Clinical Excellence, LLC;
- disclosure at your request, such as to complete transactions you undertake on the Website;
- disclosure to vendors engaged by ASCO to outsource one or more of our internal functions, products, or services, including but not limited to managing mailing lists, packaging, mailing and delivering purchases and promotional offers, consulting services, data modeling, printing, sending postal mail, and processing event registrations;
- disclosure of contact information to other ASCO members via our membership directories (the information made available in directories will not include will not include financial information, such as credit card or bank information, or social security numbers);
- disclosure of contact information to the public if you elect to participate in the Find an Oncologist Database (www.cancer.net/find-cancer-doctor);
- limited disclosure of contact information to trusted third parties to offer products and services to our members; and
- disclosure to private entities and law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate (a) to investigate or resolve possible problems or inquiries, (b) to conform to legal requirements or comply with legal process served on ASCO, (c) to protect our own business and assets, or (d) in special cases, such as a physical threat to you or others.

Please note that additional disclosure rules apply to information obtained by ASCO through the Oncology Career Center™, which is discussed further in Section 10.

Whenever ASCO discloses your PII to third parties, we will make commercially reasonable efforts to limit the information to which third parties have access and the

purposes for which they can use it, as well as to require that the recipients thereof apply the terms of this Privacy Policy to that information as if they were ASCO.

6. Your Rights to View and Correct Information Submitted Voluntarily

The tools that collect and store PII allow you to correct, update or review that information (and any preferences) by logging-in to the specific service and making the desired changes to your registration information. In most cases you may also withdraw your registration by sending us an email at privacy@asco.org. If you withdraw a registration with the Website your PII may not be deleted from our records and we may use that data for internal purposes.

7. Your Rights to Opt-out, Opt-in, or Limit Specific Uses and Disclosures of Your Personally Identifiable Information

When you register, you may be asked whether you want to receive special announcements and future newsletters by email. If you check "yes" but change your mind at any time in the future and no longer wish to receive our newsletter and other special announcements by email, you will be able to Opt-Out of these services by: (a) going to MyASCO (www.asco.org/ascov2/myasco) and selecting "Update Email Subscriptions"; (b) following the directions included at the bottom of any newsletter issue; and/or (c) sending us an email at privacy@asco.org, and we will take you off the applicable list. You may also Opt-In to receive communications from us and trusted third parties at the point of registration or by similarly following the instructions above.

You may Opt-Out of having your PII shared with trusted third parties for the purposes of offering products and services to our members by sending us an email at privacy@asco.org.

8. What Security Procedures We Use to Protect Your Information

ASCO is committed to keeping user information secure, and implements commercially reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. Access to data and technology relating to user information is password-protected and limited to authorized personnel and those vendors that require access to the information in order to furnish services to ASCO and our members. In addition, ASCO uses industry standard technology to keep users' information secure while residing on ASCO's servers.

Listed below are some of the security procedures that ASCO uses to protect your privacy:

- Require both a personal Username and a Password in order for users to access their PII.
- Use Firewalls to protect information held in our Servers.
- Closely monitor the limited number of ASCO employees who have access to

your PII.

- Require all ASCO employees to abide by our Privacy Policy and be subject to disciplinary action if they violate it.
- Back-up our systems to protect the integrity of your PII.
- Use industry-standard SSL Encryption technology for any credit card information sent over the Internet.
- Require vendors with access to PII to commit to and abide by confidentiality obligations.

Despite ASCO's efforts to protect your PII, there is always some risk that an unauthorized third party may breach our security systems or that your transmissions of information over the Internet could be intercepted by third parties. ASCO is not responsible or liable for any loss or damage of any sort arising from or relating to any breach of our security or interception of your transmissions (see Terms and Conditions of Use).

9. How the Interactive Areas of the Website Operate

As a service to our users, the Website may feature message boards, chat rooms, and/or other public forums where users can share information or where users can post questions. We may also offer online discussions moderated by medical or healthcare experts.

In addition, you may choose to use certain interactive content, tools, and services that ask you to voluntarily provide information about yourself. Some of these tools (like certain quizzes or calculators) do not retain information, while others may store information in accordance with the authorization you provide at the time you use the service or tool. Please be aware of this fact.

Any chat room, message board, forum or similar interactive service is by design open to the public and is not a private, secure service. ASCO is not responsible for the privacy of information voluntarily provided by a user in interactive areas. You should think carefully before disclosing any PII in any public forum because what you have written may be seen, disclosed to, or collected by third parties and may be used by others in ways we are unable to control or predict, including to contact you for purposes unauthorized by you.

10. The Oncology Career Center™

Because the Oncology Career Center™ (www.careers.jco.org) is a career site, it gives job seekers the option of posting their resumes to our database. There are two ways to post a resume.

Non-Searchable Submission. You can store your resume in our database, but elect during the registration process to exclude your resume from searches by potential employers. Excluding your resume from database searches means that you can use it

to apply for and respond to individual job postings, but employers will not have the ability to search for it.

Searchable Submission. During the registration process you will have the option to allow your resume to be searchable by potential employers. Selecting this option permits all parties with access to our searchable resume database to have access to your resume.

You may remove your resume from the database, and change the status of the resume from searchable to non-searchable, and vice-versa, at any time by updating your profile page on the Oncology Career Centerâ¢.

Please note that the Oncology Career Centerâ¢ is an interactive service and subject to the policies and disclaimers in Section 7 of this Privacy Policy and in the Terms and Conditions of Use. We cannot and do not guarantee that third parties will not, without our or your consent, gain access to our resume database. You hereby expressly (a) acknowledge that registered employers and other third parties who gain access to the database with or without our or your consent may retain a copy of your resume in their own files or databases, even if you subsequently change the status of your resume to non-searchable, and (b) agree that in no event shall ASCO be responsible or liable for the retention, use, duplication, distribution, or privacy of resumes in these instances.

11. Compliance with Children's Online Privacy Protection Act

We do not knowingly solicit data online from or market online to children under the age of 13.

12. Where You Can Get Questions Answered about the ASCO Privacy Policy

If you have any questions or comments regarding this Privacy Policy, please contact: privacy@asco.org. If you do not receive adequate resolution of a privacy related problem, you may write to ASCO at: 2318 Mill Road, Suite 800, Alexandria, VA 22314, Attention: General Counsel.

13. Glossary

Aggregate Information. As a website gathers individual pieces of Non-Personal Information from its users, it may combine similar data from many or all the users of the website into one big "batch." For example, the site may add up the total number of people in Peoria, Illinois, (but not their names) who are seeking information about pancreatic cancer and compare that to the number of people in Petaluma, California seeking the same information.

This sort of statistical information is called aggregate data because it reflects the habits and characteristics of a large group of anonymous people. Websites may use aggregate data or share it with business associates so that the information and services they provide best meet the needs of the users. aggregate data also helps advertisers

and sponsors on the Website know how effectively they are reaching and meeting the needs of their target audience.

Browser. Short for web browser, a browser is software application used to locate and display pages of the Internet. The popular browsers include Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Opera, and Apple Safari. Most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Click Stream Information. A record of all the pages you have visited during your visit to a particular website or the services you accessed from the site or from an email. Click Stream Information is associated with your browser and not with you personally. It records the archives of your Browser.

Cookie. A small data file that is stored on the hard drive of the computer you use to view a website. Cookies are placed by that site ("first party") or by a third party with a presence on the site, such as an advertiser using a Web Beacon, and are accessible only by the party or site that placed the Cookie on the computer (i.e. a Cookie placed on your computer by ASCO is not accessed by any other site you visit but a Cookie placed on your computer by an advertiser may be accessed by any site on which that same advertiser has a presence). Cookies can contain pieces of Personally Identifiable Information. ASCO encrypts any PII it stores in first party Cookies. These Cookies often are used to make the site easier to use. For example, if you check a box to ask that we store your Username on your computer so that you don't have to enter it each time you visit the site, it's stored in a Cookie on your computer.

Encryption. The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or Password that enables you to decrypt it. This is typically done by so called "secure computer systems."

Firewall. A system designed to prevent unauthorized access to or from a public or private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized users from accessing private portions of public networks. All messages entering or leaving the network pass through the firewall, which examines each message and blocks those that do not meet specified security criteria.

Non-Personal Information ("NPI"). Information that is not traceable back to any individual and cannot be used to identify an individual. For example, Click Stream Information is Non-Personal Information, as is information such as gender, age, city, and physical location, when not linked with other Personally Identifiable Information.

Opt-In. Means you are actively indicating your preference to participate in a program, email, feature, tool, or enhancement on a website. Typically, if you "Opt-in" you must provide certain information, usually Personally Identifiable Information, to the website or

otherwise actively indicate your choice or preference to participate in the website program. For example, if you wish to receive a newsletter by email from the *Journal of Clinical Oncology* (jco.ascopubs.org), you can enter your email address and choose the type of newsletter by checking a box next to a statement such as: "Yes, I'd like to receive the JCO Newsletters."

Opt-Out. Means that if you do not take some action you are indicating your preference to participate in a program, email, feature, tool, or enhancement on a website. Typically, if you "Opt-Out" you must uncheck a box next to a stated preference or otherwise take some indicate action to indicate your preference not to participate in a program.

Password. A secret series of characters, typically alphanumeric (meaning it consists of both letters and numbers) that enables a user to access a file, computer, or program. The user must enter its, his, or her password before the computer or system will respond to commands. The password helps ensure that unauthorized users do not access the system. In addition, data files and programs may require a password.

Ideally, the password should be something that nobody could guess. In practice, many people choose a password that is easy to remember, such as their name or their initials. This is one reason it is relatively easy to break into many computer systems.

Personally Identifiable Information ("PII"). Information that can be traced back to an individual (in contrast to Non-Personal Information and Aggregate Information). Examples of PII include your name, home address, telephone number, email address, and Social Security number.

If other pieces of information are linked to PII, they also become PII. For example, if you use a nickname to chat online and give out your real name while chatting, your nickname becomes PII when linked with other PII.

Server. A computer that provides services to other computers. A "web server" stores web site files and "serves" them to people who request them.

SSL (Secure Sockets Layer). A security protocol developed by Netscape for transmitting private information via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. All major Browsers, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and Apple Safari, support SSL, and many websites use the protocol to transmit confidential user information, such as credit card numbers. By convention, URLs that utilize an SSL connection start with https: instead of http:.

Username. A name used to gain access to a computer system or program. Usernames, and often Passwords, are required in shared systems, such as the Internet. In most such systems, users can choose their own usernames and passwords.

Web Beacons (also often referenced as "clear GIFs," "web bugs," "1-by-1 GIFs,"

"Single-Pixal GIFs," "1 x 1 Pixals" or "clear Pixals"). Tiny graphic image files, imbedded in a web page in GIF, jpeg, or HTML format, that provide a presence on the web page and send back to its home Server (which can belong to the host site, a network advertiser, or some other third party) information from the users' Browser, such as the IP address, the URL of the page on which the beacon is located, the type Browser that is accessing the site, and the ID number of any Cookies on the users' computer previously placed by that server. Web Beacons can also be used to place a Cookie on the users' Browser.

EXHIBIT G-2

Privacy Policy [1]

American Society of Clinical Oncology, Inc.

Privacy Policy

Last modified: July 2016

Contents

1. Introduction

American Society of Clinical Oncology, Inc. (hereafter "**ASCO**," "**we**," or "**us**" or "**our**") has worked hard to bring you an informative and user-friendly Website that is sensitive to concerns about privacy. We have designed this Privacy Policy to explain how and when ASCO collects, uses, and safeguards the information you provide and that we collect through our Website.

By using, accessing, or becoming a Registered User of the Website, you consent to our collection, use, and disclosure of information in accordance with this Privacy Policy.

This Privacy Policy applies to information you provide to us or that we collect automatically:

- When you visit the Website.
- Through email, text, and other electronic messages or communications between you and the Website or ASCO.
- When you interact with Website content or applications that may link to or be accessible from or on the Website and that are provided or managed by a third-party, if that content or application includes a link to this Privacy Policy.

This Privacy Policy does not apply to information:

- We collect offline or through any other means not referred to above; or
- Collected through our mobile applications, which provide dedicated non-browser based interaction between you and ASCO. Our mobile applications are governed by a separate Mobile Application Privacy Policy [2], available when you download each application.

This Privacy Policy will tell you:

- Who collects information;
- What types of information are collected and how this is done;
- How ASCO uses and discloses the information that is collected;
- Your rights to view and correct information that you voluntarily submit to us;
- Your rights to opt-out, opt-in, or limit specific uses and disclosures of your information;
- How ASCO secures your information;
- How the interactive areas of our websites operate;
- How we comply with the Children's Online Privacy Protection Act; and
- Where you can get answers to your questions about this Privacy Policy.

We hope that reading this Privacy Policy gives you a clear idea of how we manage information about you. Throughout this Privacy Policy, we have underlined various terms and hot-linked them to our Glossary (Section 16 of this Privacy Policy), or hot-linked to a relevant Section within this Privacy Policy, to help you better understand their meaning.

Please carefully review this Privacy Policy to understand our policies and practices regarding the collection, use and treatment of your information. By accessing or using our Website, you agree to the terms of this Privacy Policy. This Privacy Policy may change from time to time (see Changes to our Privacy Policy). Your continued use of the Website after we make changes is deemed to be acceptance of those changes, so please check this Privacy Policy periodically for updates.

2. Certain General Principles, Terms, and Disclaimers

This Privacy Policy does not supersede the Terms of Use [3] that govern your use of the Website. Any conflict between this Privacy Policy and the Terms of Use shall be determined in favor of the Terms of Use. Please read the Terms of Use carefully.

3. Who Collects Information Through the Website

Subject to this Privacy Policy, the Terms of Use [3], and any other rules or policies applicable to the Website, ASCO and/or certain third parties collect the information described in this Privacy Policy through the Website.

ASCO Pages and Content Managed by Third Parties

The Website contains Third Party Managed Pages from which third-party vendors may directly collect PII and other information as necessary for completing authorized transactions.

The Website also makes use of third-party Cookies, Web Beacons, Pixels, and dynamic tags, which may allow third parties to collect information about you and your activities on the Website (including Web Information) and provide you, or enable others to provide you, with advertising. (See Sections 4.a, 5 and 6 for more information.)

Links to External Sites.

Our Website provides external links to other websites in order to provide those who use the Website with a better, more fulfilling experience. Once you enter another website (whether through an advertisement, service or content link, sponsorship notice or otherwise), be aware that ASCO is not responsible for the privacy or security practices of such other sites (see also Section 17 of the Terms of Use [3]). We encourage you to look for and review the privacy statements of each and every website that you visit from our Website. You should also adjust privacy settings on your Browser or account on any third-party site to match your preferences.

4. Types of Information We Collect When You Visit Our Website

We collect several types of information from and about you when you use or visit our Website, including Personally Identifiable Information or PII, Non-Personal Information or NPI, and Web Information, as outlined in this Section.

a. NPI and Web Information. If you use the Website, regardless of whether you are a Registered User, we will collect NPI and Web Information. We collect this information automatically as you navigate through the Website, through our use of automatic data collection technologies including but not limited to first and third-party Cookies, log files, Web Beacons, Pixels, dynamic tag management, and/or through other technical means. We also collect NPI and Web Information from third parties, such as through third-party advertisements on the Website, from third parties providing services to us, and from third parties with which ASCO advertises.

Generally, the NPI and Web Information we collect about you is attached to arbitrary system names that are assigned to visitors when they enter the Website. We may, however, link your NPI or Web Information with your PII in the event that you become a Registered User. In addition, providers of third-party Cookies, Pixels, Web Beacons, and/or dynamic tags used on the Website may have the ability to both link your activities on the Website (including Web Information) with information collected about you elsewhere on the Internet or otherwise in their possession and to use it for their own business purposes, including to provide you with advertising. (See Section 5 for more information on third-party Cookies.)

b. PII. We collect PII directly from you when you provide it to us, such as in the following ways:

- Information that you provide by filling out forms on our Website. This includes information provided at the time of registering as a Registered User of the Website, updating your registration or profile information, subscribing or unsubscribing to any of our services, posting material or comments, providing feedback, or requesting further information or services.
- When you report a problem with our Website.
- Records and copies of your correspondence (including email addresses) when you contact us.
- Your responses to surveys that we might ask you to complete for research purposes.
- Details of transactions you carry out through our Website and of the fulfillment of your orders with us,

including account balances and purchasing activity. You may be required to provide information sufficient for us to collect payment for registrations, membership, purchases, subscriptions, or other e-commerce transactions authorized by you, which may include but not be limited to your name, address, email address, credit or debit card information, and other information required to process payment through PayPal or other third-party mechanisms.
- When you use location-specific searches or directories we provide, such as our iDirectory or Find a Cancer Doctor Database.

If you are submitting PII on behalf of others in your family, business or other organization for registration purposes or otherwise, you represent that you have their permission, agreement and full authorization to provide this information to us. We reserve the right (a) to ask you to provide evidence of your authority at any time during, or even after, the submission process and (b) to contact those individuals to confirm your authority at any time. If we determine that your authority has not been properly obtained, we may immediately and without notice to you discontinue your authorized use of those features of the Website for which you have registered.

If you visit the Website through a link from an email newsletter sent by ASCO, our system will log information, including your email address, which links you click through from the e-mail to the Website, the date and time of your click-through, the name of the link or source from which the message was sent, the tracking URL number, and the destination page.

c. Registered Users. Some features on the Website may require you to register as a Registered User and to receive our authorization before you can use those particular features, including forums, mailing lists, meeting registrations, subscriptions, and other services. In order for you to register and use those features, we may require that you provide us with certain PII and other information about you or your business. This PII and other information may include names, addresses, e-mail addresses, telephone numbers, fax numbers, education and certifications, areas of specialty, credit card numbers (in relation to certain features), and other forms of PII . While you may use some of the functionality of the Website without becoming a Registered User, many specific tools and services on the Website require registration and your submission of PII.

Once we have authorized you as a Registered User, we may provide you with a customer identification number and you may be required to select a unique Username and Password. Generally, you will be able to change your Password and update any PII you have given us (instructions on how to make these changes can be found in Section 7 of this Privacy Policy).

If you use Website services or features as a Registered User, you acknowledge and also consent to our tracking of your activities and use of the Website under your Username and/or customer identification number. ASCO may use such information to improve user experience, in order to confirm and fill orders, maintain quality control and contact you concerning your orders, transactions, or subscriptions, as well as for other uses consistent with this Privacy Policy.

If you have access to the Website as a designated representative of a business, ASCO may terminate your right to use the Website upon notification that you are no longer a designated representative for that business.

d. Posts to Our Website. You also may provide information to be published or displayed (hereinafter, "**posted**") on public areas of the Website, or transmitted to other users of the Website or third parties (collectively, "**User Contributions**"). Your User Contributions are posted on and transmitted to others at your own risk. Although we limit access to certain pages, please be aware that no security measures are perfect or impenetrable. Additionally, we cannot control the actions of other users of the Website with whom you may choose to share your User Contributions. Therefore, we cannot and do not guarantee that your User Contributions will not be viewed or used by unauthorized persons.

5. How We Use Your Information

We use the information you provide to us and the information we collect automatically to improve our services and your experience with the Website. Our use of your information and any communications from you to us through the Website will in each case be in a manner consistent with the Terms of Use [3] and this Privacy Policy.

Use of Your NPI and Web Information. The NPI and Web Information we automatically collect from you is generally used to render, administer, and improve the Website, our services, and our business. It helps us to improve our Website and to deliver a better and more personalized service. Purposes for which we may use such information include, but are not limited to, the following:

- To present our Website and its contents to you.
- To help dynamically generate content on web pages or in newsletters.
- To statistically monitor how many people are using the Website.
- To track generic user behavior (for example, through Web Information).
- To monitor how many people open our emails.
- To help us evaluate the purpose for which our users undertake certain activities, including those listed immediately above.
- To determine the popularity of certain content.
- To restrict underage use of our services.
- To speed up your searches.
- To enable us and our advertisers and social media partners to display advertisements to appropriate target audience(s) and for other marketing and advertising purposes, including Online Behavioral Advertising.
- To remember you when you visit the Website, to facilitate your log-in and navigation, and as session timers. To store information about your preferences, allowing us to customize our Website according to your individual interests.
- To locate member practices and practice locations for non-members, to search for members in our iDirectory and in our Find a Cancer Doctor Database, to offer institutional licensing, and to comply with location-specific laws through the use of geolocation data.
- For other commercially reasonable purposes, including measuring advertising and promotional effectiveness and assessing which areas of the Website to remarket to you after you leave our site.

Use of Your PII. We use PII, and any data that you provide, personal or otherwise, to provide our products and services. Examples of the ways in which we may use PII include but are not limited to the following:

- To present our Website and its contents to you.
- To respond to your questions.
- To remember you when you visit the Website, to facilitate your log-in and navigation, and as session timers. To store information about your preferences, allowing us to customize our Website according to your individual interests.
- To provide you with products, services or subscriptions you select.
- To contact you regarding ASCO events or other news.
- To provide you with information you request.
- To send and manage surveys.
- To advise you of products or services that may be available through ASCO.
- To notify you about Website maintenance, updates, changes, and new features, including products or services we offer or provide through the Website.
- To notify you regarding your account or subscription, including expiration and renewal notices.

- To contact you as needed to address a suspected violation of the Terms of Use, this Privacy Policy, or any other rules or policies applicable to the Website.
- To inform you of significant changes to this Privacy Policy.
- To manage membership and volunteer functions.
- To display content we think may be of interest to you and otherwise help us customize what you see when you visit the Website.
- To allow you to participate in interactive features on our Website.
- To solicit user feedback to assess user-satisfaction or other needs and interests.
- To help us in creating new tools, features, and services.
- To confirm or fulfill purchase and registration requests.
- To locate member practices and practice locations for non-members, to search for members in our iDirectory and in our Find a Cancer Doctor Database, to offer institutional licensing, and to comply with location-specific laws through the use of geolocation data.
- To enable us and our advertisers to display advertisements to appropriate target audience(s) and for other marketing and advertising purposes, including Online Behavioral Advertising.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- In any way we may describe when you provide the information.
- To render, administer, and improve the Website, our services, and our business in other commercially reasonable ways.
- For any other purpose with your consent.

E-Commerce Transactions. When you place an order online with us, register for a conference, pay your dues electronically, or otherwise enter into an e-commerce transaction with us, we collect and transfer to a third-party vendor information sufficient for us to collect payment for these e-commerce transactions, which may include but not be limited to your name, address, email address, credit or debit card information, and other information required to process payment through PayPal or other third-party mechanisms.

Use of Third Party Cookies and Other Tracking Technologies. The Website makes use of automatic data collection technologies including first and third-party Cookies, log files, Web Beacons, Pixels, dynamic tags, and/or other technical means. We may use these technologies to collect information about your online activities over time and across third party websites or other online services in order to deliver content and advertising tailored to your interests, both on the Website and on third-party websites (including but not limited to search engines and social media websites). This practice is commonly known as Online Behavioral Advertising.

The third parties who provide us with third-party Cookies, Web Beacons, Pixels, dynamic tags, and/or other tracking technologies, may use these technologies to collect information about you when you use the Website in order to provide you with advertising based on your visit to the Website. Third parties may have the ability to link the information they collect about you when you use the Website with other information they collect about you elsewhere on the Internet, including but not limited to your PII or information about the device you are using. Third parties may also collect information about your online activities over time and across different websites and other online services and may use this information to provide you with Online Behavioral Advertising or other targeted content.

We encourage you to research and learn about Cookies mand other technical means, including Web Beacons, Pixels, and dynamic tags, through which information about you may be collected through the websites you visit. For more information about how to opt out of the use of some of these technologies, see Choices About How We Use and Disclose Your Information.

Social Networking.

ASCO may maintain a presence on third-party social networking sites such as Facebook, LinkedIn, Twitter, and others. ASCO does not control or have responsibility for the collection, tracking, use, or disclosure of your information (including your PII, NPI and Web Information) gathered through these social networking sites, including through the ASCO pages or profiles within those sites, or otherwise as a result of your participation in social networking sites. Third-party social networking sites and advertisers on these sites, including on the ASCO pages or profiles within these sites, are not obligated to follow or apply this Privacy Policy or the Terms of Use. If you have any questions about an advertisement or other targeted content, you should contact the responsible social networking provider directly.

6. How We Disclose Your Information

Disclosure of NPI and Aggregate Information. ASCO may provide NPI or Aggregate Information about our users and information that does not identify any individual to third parties without restriction. For example, we might inform third parties regarding the number of users of the Website and the activities they conduct while on the Website. We might, for example inform a pharmaceutical company (that may or may not be a sponsor of the Website), that "30% of our users live east of the Mississippi" or that "25% of our users have tried alternative medicine."

Disclosure of Personally Identifiable Information. We may disclose PII that we collect or that you provide as described in this Privacy Policy:

- To our subsidiaries and corporate affiliates, including the Conquer Cancer Foundation (www.conquercancerfoundation.org [4]), CancerLinQ, LLC (www.cancerlinq.com [5]), and QOPI Certification Program, LLC (http://www.instituteforquality.org [6]).
- To contractors, service providers, and other third parties we use to support our business, internal functions, products, or services, including but not limited to managing mailing lists, packaging, mailing and delivering purchases and promotional offers, consulting services, data modeling, printing, sending postal mail, outreach efforts, and processing event registrations.
- To fulfill the purpose for which you provide it. For example, to complete transactions you undertake on the Website.
- To other ASCO Members if you choose to participate in our membership directories (the information made available in directories will include contact information and will not include financial information, such as credit card or bank information).
- If you are a medical provider and you elect to participate in the Find A Cancer Doctor Database (www.cancer.net/find-cancer-doctor [7]) and authorize the disclosure of your contact information through that Database, or if you are an ASCO Member, your contact information may be disclosed to members of the public accessing that Database. You may elect to make your information private or cease participation in the Database at any time by contacting ASCO Customer Service (https://www.asco.org/contact-us [8]).
- To our advertising and social media partners, to enable us and our partners to provide advertisements to appropriate target audience(s).
- To private entities and law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate (a) to investigate or resolve possible problems or inquiries, (b) to conform to legal requirements or comply with any court order, law or legal process, including responding to any government or regulatory request, (c) to protect our own rights, property or safety of ASCO, our customers, or others, (d) to enforce or apply our Terms of Use and any other agreements, including for billing and collection purposes, or (d) in special cases, such as a physical threat to you or others.
- For any other purpose(s) disclosed by us when you provide the information.

- With your consent.

Please note that additional disclosure rules apply to information obtained by ASCO through the Oncology Career Center™, which is discussed further in Section 10.

In the event of a change of control of ASCO (or the Website or any portion thereof), such as through a merger, sale, consolidation, transfer of substantial assets, reorganization or liquidation, or other similar transaction, ASCO reserves the right to transfer, sell, or assign to third parties any information we have collected.

Disclosure of Information to Third-Party Vendors and Service Providers. ASCO has engaged third-party vendors and service providers to provide services in connection with the Website, outreach for our programs and services, and to help us manage our web presence and allow us to better serve our users. In addition, some of the content and services on the Website, including advertisements, are served by third parties, including advertisers, ad networks and servers, content providers, and technology and application providers. We may share PII or other information with these third-party vendors and service providers as necessary so that they may provide the services for which they have been engaged. PII and other information submitted to ASCO through Third Party Managed Pages are also shared with the relevant third-party vendor as necessary for completing authorized transactions.

7. Your Rights to View and Correct Information You Provide to Us

If you are a Registered User of the Website, you can review, correct and change your PII (and any preferences) by logging into the Website and visiting your account profile page.

You may also send us an email at privacy@asco.org [9] to request access to, correct or delete any PII that you have provided to us. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect. If you withdraw your registration as a Registered User of the Website we may retain your PII in our records and we may continue to use and disclose that data in a manner consistent with this Privacy Policy, unless you request deletion of it.

If you delete your User Contributions from the Website, copies of your User Contributions may remain viewable in cached and archived pages, or might have been copied or stored by other Website users. Please refer to our Terms of Use [3] for information relating to the proper access and use of User Contributions.

8. Your Choices About How We Use and Disclose Your Information

You are able to control your information in the following ways:

Promotional Offers from ASCO and Third Parties. When you register, you may be asked whether you want to receive special announcements and future newsletters by email. If you check “yes” but change your mind at any time in the future and no longer wish to receive our newsletter and other special announcements by email, you will be able to Opt-Out of these services by: (a) going to Email Subscriptions (apps.asco.org/EmailPreferences [10]) and selecting “Update Email Subscriptions”; (b) following the directions included at the bottom of any newsletter issue; and/or (c) sending us an email at privacy@asco.org [9], and we will take you off the applicable email list. You may also Opt-In to receive email communications from us and trusted third parties at the point of registration or by similarly following the instructions above. This Opt-Out does not apply to information provided to us as a result of a product or service purchase, product service communications, or other transactions.

Cookies. You can set your browser to refuse all or some browser Cookies, or to alert you when Cookies are being sent. Your Browser can be set to reject all Cookies. A “help” section of most Browsers’ toolbars usually

offers instructions on how to reset the browser to reject Cookies. To learn how you can manage your Flash Cookie settings, visit the Flash player settings on Adobe's website. If you disable or refuse Cookies, please note that some parts of the Website may not function properly, or may no longer be accessible.

9. How We Secure and Dispose of Your Information

ASCO has implemented reasonable security measures designed to secure your PII from accidental loss and from unauthorized access, use, alteration, and disclosure. Access to data and technology relating to user information is password-protected and limited to authorized personnel and those vendors that require access to the information in order to furnish services to ASCO and our members. In addition, ASCO uses industry standard technology to keep users' information secure while residing on ASCO's servers. However, despite these measures, our IT systems could be compromised by parties seeking unauthorized access to our data or users' data, by a technological malfunction or by an error by an employee, vendor or contractor. In addition, the transmission of information via the Internet could be intercepted by third parties. As a result, our efforts to protect our data and users' data from unauthorized access may be unsuccessful and we cannot assure you that the security measures we have adopted will provide absolute certainty. By using, accessing or become a Registered User of the Website, you agree that ASCO is not responsible or liable for any loss or damage of any sort arising from or relating to any breach of our security, circumvention of any privacy settings or security measures, or interception of your transmissions (see Terms of Use [3]). Any transmission by you is at your own risk.

When you provide PII and credit card information for e-commerce transactions, this information is encrypted using industry-standard SSL Encryption technology before being sent over the Internet. We submit to the appropriate credit card clearinghouse only the information necessary to collect payment. All credit card information retained by ASCO, including credit card numbers if you elect to store them on your account, is compliant with Payment Card Industry Data Security Standards.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Website, you are responsible for keeping this password confidential. We ask you not to share your password with anyone. We urge you to be careful about giving out information in public areas of the Website like message boards. The information you share in public areas may be viewed by any user of the Website.

Information related to your ASCO membership will be retained unless you contact us at privacy@asco.org [9] to request its deletion. Other information you provide to us and that we collect from you will be retained for no longer than reasonably necessary to fulfill the purposes for which it was obtained, or for a period specifically required by law or regulation. Your information will be disposed of in a manner that seeks to prevent loss, theft, misuse, or unauthorized access.

10. How the Interactive Areas of the Website Operate

As a service to our users, the Website may feature message boards, chat rooms, and/or other public forums where users can share information or where users can post questions. We may also offer online discussions moderated by medical or healthcare experts.

In addition, you may choose to use certain interactive content, tools, and services that ask you to voluntarily provide information about yourself. Some of these tools (like certain quizzes or calculators) do not retain information, while others may store information in accordance with the authorization you provide at the time you use the service or tool. Please be aware of this fact.

Any chat room, message board, forum or similar interactive service is by design open to the public and is not a

private, secure service. ASCO is not responsible for the privacy of information voluntarily provided by a user in interactive areas. You should think carefully before disclosing any PII in any public forum because what you have written may be seen, disclosed to, or collected by third parties and may be used by others in ways we are unable to control or predict, including to contact you for purposes unauthorized by you.

11. The Oncology Career Center™

Because the Oncology Career Center™ (careercenter.asco.org [11]) is a career site, it gives job seekers the option of posting their resumes to our database. There are two ways to post a resume.

Non-Searchable Submission. You can store your resume in our database, but elect during the registration process to exclude your resume from searches by potential employers. Excluding your resume from database searches means that you can use it to apply for and respond to individual job postings, but employers will not have the ability to search for it.

Searchable Submission. During the registration process you will have the option to allow your resume to be searchable by potential employers. Selecting this option permits all parties with access to our searchable resume database to have access to your resume.

You may remove your resume from the database, and change the status of the resume from searchable to non-searchable, and vice-versa, at any time by updating your profile page on the Oncology Career Center™.

Please note that the Oncology Career Center™ is an interactive service that uses Cookies and tracking technologies, subject to the policies and disclaimers in Section 5 of this Privacy Policy and in the Terms of Use [3]. We cannot and do not guarantee that third parties will not, without our or your consent, gain access to our resume database. You hereby expressly (a) acknowledge that registered employers and other third parties who gain access to the database with or without our or your consent may retain a copy of your resume in their own files or databases, even if you subsequently change the status of your resume to non-searchable, and (b) agree that in no event shall ASCO be responsible or liable for the retention, use, duplication, distribution, or privacy of resumes in these instances.

12. Children Under the Age of 13 - Compliance with Children's Online Privacy Protection Act

Our Website is not intended for children under 13 years of age. No one under age 13 may provide any PII to or on our Website. We do not knowingly collect personal information from children under the age of 13. If we learn we have collected or received personal information from a child under 13 without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under 13, please contact us at privacy@asco.org [9].

13. Your California Privacy Rights

California Civil Code Section 1798.83 permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send us an email to privacy@asco.org [9] or write us at American Society of Clinical Oncology, Inc., 2318 Mill Road, Suite 800, Alexandria, Virginia 22312, Attn: Privacy Officer.

California Do Not Track Disclosure. ASCO does not have a mechanism in place for responding to browser "do not track" signals or other similar mechanisms used to limit collection of information for use in Online Behavioral Advertising.

14. Changes to our Privacy Policy

ASCO reserves the right to make changes to this Privacy Policy at any time by posting revised terms directly to this page. Amendments to this Privacy Policy are effective when posted and the date on which the Privacy Policy was last revised is identified at the top of this page. ASCO does not have an obligation to provide further notice of any changes and it is each user's responsibility to monitor and review updates to this Privacy Policy. If we make material changes to how we treat our users' PII, we will notify you by email to the primary email address specified in your account, to the extent you are a Registered User with us and provided a deliverable email address. You are responsible for ensuring that we have an up-to-date, active and deliverable email address for you. Your continued use of the Website after the posting of amendments will be deemed acceptance of the changes to the Privacy Policy.

15. Where You Can Obtain Answers about the ASCO Privacy Policy

If you have any questions or comments regarding this Privacy Policy and our privacy practices, please contact: privacy@asco.org [9]. If you do not receive adequate resolution of a privacy related problem, you may write to ASCO at: 2318 Mill Road, Suite 800, Alexandria, VA 22314, Attention: General Counsel.

16. Glossary

Aggregate Information. Non-Personal Information, or Personally Identifiable Information that has been de-identified, that is combined with similar data related to more than one individual to form aggregated information. For example, the site may add up the total number of people in Peoria, Illinois, (but not their names) who are seeking information about pancreatic cancer and compare that to the number of people in Petaluma, California seeking the same information. This sort of statistical information is called Aggregate Information because it reflects the habits and characteristics of a large group of anonymous people. Websites may use aggregate data or share it with third parties so that the information and services provided best meet the needs of their users. Aggregate Information also helps advertisers and sponsors on the Website know how effectively they are reaching and meeting the needs of their target audience.

Browser. Short for web browser, a browser is a software application used to locate and display pages of the Internet. The popular browsers include Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Opera, and Apple Safari. Most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Cookie (or browser cookie). A small data file that is stored on the computer you use to view a website. Cookies are placed by that site ("**first party**") or by a third party with a presence on the site ("**third party**"), such as an advertiser using a Web Beacon, and are generally accessed only by the party or site that placed the Cookie on the computer (i.e. a Cookie placed on your computer by ASCO is generally not accessed by any other site you visit but a Cookie placed on your computer by an advertiser may be accessed by any site on which that same advertiser has a presence). Cookies can contain pieces of Personally Identifiable Information. Cookies often are used to make the site easier to use. For example, if you check a box to ask that we store your Username on your computer so that you don't have to enter it each time you visit the site, it's stored in a Cookie on your computer. Cookies may be persistent (meaning that they are saved on your computer even after you close your Browser and may be accessed at a later time) or non-persistent (meaning that they are deleted when you close your Browser). Cookies may be "essential" for the use of a website, such as for example session-id cookies, authentication cookies or user centric security cookies, or "non-essential" for the use of a website, such as for example, third party advertising cookies or other tracking cookies.

Encryption. The translation of data into a secret code. Encryption is one way to achieve data security. To read

an encrypted file, you must have access to a secret key or Password that enables you to decrypt it. This is typically done by so called "secure computer systems."

Non-Personal Information ("NPI"). Information that may relate to an individual but does not identify that individual. For example, Web Information is Non-Personal Information, as is information such as gender, age, city, and physical location, when not linked with other Personally Identifiable Information. NPI may be "re-identified" through certain processes by linking it to PII relating to the same individual.

Online Behavioral Advertising. The practice of using online tracking technologies such as Cookies and Web Beacons to collect information, including Web Information, about a user's online activities over time and/or across third-party websites or other online services in order to deliver advertising and content tailored to the user's interests.

Opt-In. An option that allows you to actively indicate your preference to participate in a program, email, feature, tool, or enhancement on a website. Typically, if you "Opt-in" you must provide certain information, usually Personally Identifiable Information, to the website or otherwise actively indicate your choice or preference to participate in the website program. For example, if you wish to receive a newsletter by email from the *Journal of Clinical Oncology* (jco.ascopubs.org [12]), you can enter your email address and choose the type of newsletter by checking a box next to a statement such as: "Yes, I'd like to receive the JCO Newsletters."

Opt-Out. An option that allows you to actively indicate your preference not to participate in a program, email, feature, tool, or enhancement on a website. Typically, if you "Opt-Out" you must uncheck a box next to a stated preference or otherwise take some action to indicate your preference not to participate in a program. Failure to opt-out typically means that you will, by default, participate in the program, feature, tool or enhancement.

Password. A secret series of characters, typically alphanumeric (meaning it consists of both letters and numbers), that enables a user to access a file, computer, or program. The user must enter its, his, or her password before the computer or system will respond to commands. The password helps ensure that unauthorized users do not access the system. In addition, data files and programs may require a password. A password should be something that nobody but the user could guess.

Personally Identifiable Information ("PII"). Information that identifies or is uniquely associated with an individual, such as a name, tax payer identification number, home address, telephone number, email address, Social Security number, or credit card number.

Pixel. See the definition of "Web Beacons".

Posted. Defined in Section 4.d of this Privacy Policy.

Registered User. Users who register to use particular features of the Website that require registration and, in some instances, the submission of PII, including but not limited to forums, mailing lists, meeting registrations, subscriptions, and other services, as described in Section 4.c of this Privacy Policy.

Server. A computer that provides services to other computers. A "web server" stores web site files and "serves" them to people who request them. Servers may belong to ASCO or to other affiliated or non-affiliated entities.

SSL (Secure Sockets Layer). A security protocol developed by Netscape for transmitting private information via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. All major Browsers, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and Apple Safari, support SSL, and many websites use the protocol to transmit confidential user information, such as credit card numbers. By convention, URLs that utilize an SSL connection start with https: instead of http:.

Third Party Managed Pages. Certain pages of the webist, such as registration, job search, journal, and submission pages that are managed by third parties, and from which third party vendors may directly collect PII and other information as necessary for completing authorized transactions, including but not limited to the *Journal of Clinical Oncology* website (jco.ascopubs.org [12]), the *Journal of Oncology Practice* website (jop.ascopubs.org [13]), the Oncology Career Center™ website (careercenter.asco.org [11]), portions of the Career Opportunities at ASCO page (www.asco.org/about-asco/careers-asco [14]), portions of ASCO in Action (ascoaction.asco.org [15]), the Conquer Cancer Foundation Donation page, the TAPUR page, the QOPI page, the Cohort site, abstract submission, meeting or conference registration, voting, and shopping cart pages.

Username. A name used to gain access to a computer system or program. Usernames, and often Passwords, are required in shared systems, such as the Internet. In most such systems, users can choose their own usernames and passwords.

User Contributions. Defined in Section 4.d of this Privacy Policy.

Web Beacons or **Pixels** (also often referred to as "clear GIFs," "pixel tags," "1-by-1 GIFs," "Single-Pixel GIFs," "1 x 1 Pixels" or "clear Pixels"). Pages of the Website and our e-mails may contain small electronic files known as web beacons that permit us and/or third parties to collect Web Information during your visit to the Website. For example, Web Beacons may be used to count the number of users who have visited a page or opened an e-mail and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity). Web Beacons send information back to their home Server (which can belong to the host site, a network advertiser, or some other third party) from the users' Browser, such as the IP address, the URL of the page on which the beacon is located, the type of Browser that is accessing the site, and information stored in any Cookies on the users' computer previously placed by that Server. Web Beacons can also be used to place a Cookie on the users' Browser. Third parties who provide us with web beacons or pixels may have the ability to link the information they collect about you when you use the Website with other information they collect about you elsewhere on the Internet, including but not limited to your PII or information about the device you are using.

Web Information. Information about your activities on the Website and the technology you use to access the Website, including information about the date and time you visit the Website, the services you accessed from the site or from an email, how you arrive at the Website (through referral or exit links or otherwise), which pages you view, any files you download, for how long you visit the Website and view pages, when you last visited the site, your IP address, your location, your connection, your search terms, the type of Browser and operating system you use, mobile device make and model, mobile device carrier information, and mobile device support specifications such as screen size, color, video, and image support.

Website. Collectively, the ASCO website (www.asco.org [16]), the Cancer.Net website (www.cancer.net [17]), the *Journal of Clinical Oncology* website (jco.ascopubs.org [12]), the *Journal of Oncology Practice* website (jop.ascopubs.org [13]), the *Journal of Global Oncology* website (jgo.ascopubs.org [18]), the Oncology Career Center™ website (careercenter.asco.org [11]), the Quality Oncology Practice Initiative website (http://www.instituteforquality.org [6]), the ASCO University website (university.asco.org [19]), the CancerProgress.net website (www.cancerprogress.net [20]), the ASCO Connection website (www.connection.asco.org [21]), the ASCO Photo Gallery (photos.asco.org [22]), the TAPUR Study website (www.tapur.org)

[23], the ASCO University Meeting Library website (www.meetinglibrary.asco.org [24]), the ASCO in Action website (www.ascoaction.asco.org [25]), and any other online functionalities or services included in the websites operated by ASCO, but excluding our mobile applications, or “apps.”

Links
[1] http://www.cancer.net/es/node/25319
[2] http://www.asco.org/about-asco/legal/mobile-app-privacy-policy
[3] http://www.cancer.net/node/25403
[4] http://www.conquercancerfoundation.org
[5] http://www.cancerlinq.com
[6] http://www.instituteforquality.org
[7] http://www.cancer.net/find-cancer-doctor
[8] https://www.asco.org/contact-us
[9] mailto:privacy@asco.org
[10] http://apps.asco.org/EmailPreferences
[11] http://careercenter.asco.org
[12] http://jco.ascopubs.org
[13] http://jop.ascopubs.org
[14] http://www.asco.org/about-asco/careers-asco
[15] http://ascoaction.asco.org
[16] http://www.asco.org
[17] http://www.cancer.net
[18] http://jgo.ascopubs.org
[19] http://university.asco.org
[20] http://www.cancerprogress.net
[21] http://connection.asco.org
[22] http://photos.asco.org
[23] http://www.tapur.org
[24] http://meetinglibrary.asco.org
[25] http://www.ascoaction.asco.org

EXHIBIT H-1

MELANOMA RESEARCH FOUNDATION

Privacy Policy

Melanoma Research Foundation Privacy Policy

The Melanoma Research Foundation ("**MRF**" or "**we**," "**us**," or "**our**") is committed to protecting your privacy. We have prepared this Privacy Policy to describe to you our practices regarding the Personal Data (as defined below) we collect from users of our website located at www.melanoma.org and related services (collectively, the "**Service**").

1. User Consent. By submitting Personal Data through the Service, you agree to the terms of this Privacy Policy and you expressly consent to the processing of your Personal Data in accordance with this Privacy Policy.

2. A Note to Users Outside of the United States. Your Personal Data may be processed in the country in which it was collected and in other countries, including the United States, where laws regarding processing of Personal Data may be less stringent than the laws in your country. We adhere to the United States / European Union Data Protection Safe Harbor Arrangement, which can be located at http://www.export.gov/safeharbor/.

3. Types of Data We Collect. The MRF collects Personal Data and Anonymous Data from you when you send us information or communications and/or when you use the Service. "**Personal Data**" means data that allows someone to identify or contact you, including, for example, your name, address, telephone number, e-mail address, as well as any other non-public information about you that is associated with or linked to any of the foregoing data. "**Anonymous Data**" means data that is not associated with or linked to your Personal Data; Anonymous Data does not permit the identification of individual persons. We collect Personal Data and Anonymous Data, as described below.

3.1 Personal Data You Provide to Us. We collect Personal Data from you, such as your first and last name, e-mail and mailing addresses, and phone number, when you do any of the following:

- Donate money through the Service;
- Sign up for an online newsletter or other informational or promotional communications;
- Sign up as a volunteer or member;
- Create or modify your account on the Service;

- Provide us feedback or contact us via e-mail or the Service;
- Elect to post or submit messages, questions, comments, or other content to the Service; or
- Provide information at any point in the Service that states that Personal Data is being collected.

3.2 Personal Data Collected via Technology. To make our Service more useful to you, we collect Personal Data from you through our servers (which may be hosted by a third party service provider) and/or third party tools, including:

- Browser type, operating system, and Internet Protocol (IP) address (a number that is automatically assigned to your computer when you use the Internet, which may vary from session to session);
- Date/time stamp for your visit; and
- Cookies (as defined below) and navigational data like Uniform Resource Locators (URL) to gather information regarding the date and time of your visit and the solutions and information for which you searched and which you viewed. Like most Internet services, we automatically gather this Personal Data and store it in log files each time you visit the Service. "Cookies" are small pieces of information that a website sends to your computer's hard drive while you are viewing a web site. We may use both session Cookies (which expire once you close your web browser) and persistent Cookies (which stay on your computer until you delete them) to provide you with a more personal and interactive experience on our website. Persistent Cookies can be removed by following Internet browser help file directions. If you choose to disable Cookies, some areas of our website may not work properly.

4. Use of Your Data

4.1 General Use. In general, Personal Data you submit to us is used either to respond to requests that you make, or to aid us in serving you better. The MRF uses your Personal Data in the following ways:

- Provide improved administration of the Service;
- Improve the quality of experience when you interact with the Service;
- Facilitate the creation of and secure your account on our network;
- Send you administrative e-mail notifications, such as security or support and maintenance advisories;
- Respond to your inquiries related to employment opportunities, questions about melanoma, or other requests;
- Respond to comments or messages you post on the Service;
- Thank you for your donation; and
- To send you promotional communications or our online newsletter.

4.2 Creation of Anonymous Data. We may create Anonymous Data records from Personal Data by excluding information (such as your name) that makes the data personally identifiable to you. We use this Anonymous Data to analyze request and usage patterns so that we may enhance the content of the Service and improve site navigation. The MRF reserves the right to use and disclose Anonymous Data in its sole discretion.

4.3 Feedback. If you provide feedback to us on the Service, we may use such feedback for any purpose; provided we will not associate such feedback with your Personal Data. The MRF will collect any information contained in such communication and will treat the Personal Data in such communication in accordance with this Privacy Policy.

5. Disclosure of Your Personal Data

5.1 Affiliates. Although we currently do not have a parent company, any subsidiaries, joint ventures, or other companies under a common control (collectively, "**Affiliates**"), we may in the future. We may share some or all of your Personal Data with these Affiliates, in which case we will require our Affiliates to honor this Privacy Policy. If another company acquires our company or our assets, that company will possess the Personal Data collected by it and us and will assume the rights and obligations regarding your Personal Data as described in this Privacy Policy.

5.2 Other Disclosures. Regardless of any choices you make regarding your Personal Data (as described below), the MRF may disclose Personal Data if it believes in good faith that such disclosure is necessary to (a) comply with relevant laws or to respond to subpoenas or warrants served on the MRF; or (b) protect or defend the rights or property of the MRF or users of the Service.

6. Third parties

6.1 Personal and/or Anonymous Data Collected by Third Parties. We may receive Personal and/or Anonymous Data about you from other sources like telephone or fax, or from companies that provide services, such as, but not limited to, co-branded websites or services and online donations ("Third Party Companies"). Our Third Party Companies may supply us with Personal Data, such as your name, address, and email address. We may add this information to the information we have already collected from you via the Service to improve the Service, to send you a thank you, or to send you our online newsletter. Our provision of a link to any other website or location, such as, but not limited to, donation processing websites, is for your convenience and does not signify our endorsement of such other website or location or its contents. When you click on such a link, you will leave our site and go to another site. During this process, another entity may collect Personal Data or Anonymous Data from you. We have no control over, do not review, and cannot be responsible for, these outside websites or their content. Please be aware that the terms of this Privacy Policy do not apply to these outside websites or content, or to any collection of data after you click on links to such outside websites.

6.2 Disclosure to Third Party Service Providers and Third Party Companies. Except as otherwise stated in this policy, we do not generally sell, trade, share, or rent the Personal Data collected from our services to other entities. However, we may share your Personal Data with third party service providers to provide you with the Service; to conduct quality assurance testing; to facilitate creation of accounts; to provide technical support; to send you our online newsletter, to enable online donations, or to provide other services. These third party service providers are required not to use your Personal Data other than to provide the services requested by the MRF. You expressly consent to the sharing of your Personal Data with our contractors and other service providers for the sole purpose of providing services to you. We do not sell or share your Personal Data with Third Party Companies.

6.3 Links to Other Sites. Our Service contains links to Internet sites maintained by third parties.

These links are provided for your reference only. We do not control, operate or endorse in any respect information, products, or services on such third-party sites and are not responsible for their content. Many third-party sites have their own privacy policies that differ from ours. This Privacy Policy only covers our Service and does not cover any other site.

7. Donation Information. If you choose to donate to the MRF via our website, we or our third-party service provider will collect your payment information. To make any payments via the Service you will be required to give us, or our third party service providers a valid credit card number and associated payment information at the time you are required to make such payments, including all of the following: (1) your name as it appears on the card, (2) the credit card type, (3) the date of expiration of your credit card, (4) any activation numbers or codes needed to charge your card, and (5) billing address. You agree that no additional notice or consent is required before we (or our third party service providers) invoice your credit card provided to us for all amounts payable. We use our partners and third-party service providers to assist with billing and payment processes. Any Personal Data you provide to such third-party service provider will be subject to that third-party service provider's privacy policy and website terms of use, and not to this Privacy Policy or our terms of use.

8. Your Choices Regarding Your Personal Data

8.1 Choices. We offer you choices regarding the collection, use, and sharing of your Personal Data. We may periodically send you free newsletters and e-mails that directly promote the use of the Service and /or provide you information on our goals and progress. When you receive newsletters or promotional communications from us, you may indicate a preference to stop receiving further communications from us and you will have the opportunity to "opt-out" by following the unsubscribe instructions provided in the e-mail you receive or by contacting us directly (please see contact information below). Should you decide to opt-out of receiving future mailings, we may share your e-mail address with third parties to ensure that you do not receive further communications from third parties. Despite your indicated e-mail preferences, we may send you administrative e-mails regarding the Service or notices of any updates to our terms of use or Privacy Policy. You may not opt-out of these communications, which are not promotional in nature, but if you do not wish to receive these announcements, you have the option to deactivate your membership account.

8.2 Changes to Personal Data. You may change any of your Personal Data in your account by sending an e-mail to us at the e-mail address set forth below. You may request deletion of your Personal Data by us, but please note that we may be required (by law or otherwise) to keep this information and not delete it (or to keep this information for a certain time, in which case we will comply with your deletion request only after we have fulfilled such requirements). When we delete any information, it will be deleted from the active database, but may remain in our archives.

9. Shared or Public Areas of the Service. Please be aware that if you enter any Personal Data into public or shared sections of the Service, such as, but not limited to, the chat room and bulletin board, your Personal Information will be displayed to anyone who has access to these sections of the Service. The MRF has no control over, and will have no liability to you regarding, other users' use or disclosure of such Personal Data.

10. Security of Your Personal Data. The MRF is committed to protecting the security of your Personal Data. We use a variety of industry-standard security technologies and procedures to

help protect your Personal Data from unauthorized access, use, or disclosure. Despite these measures, you should know that the MRF cannot fully eliminate security risks associated with Personal Data and cannot guarantee that unauthorized access to your information will never occur.

11. Contact Information. The MRF welcomes your comments or questions regarding this Privacy Policy. Please e-mail us at info@melanoma.org or contact us at the following address or phone number:

Melanoma Research Foundation
Attn: Website Coordinator
1411 K Street NW Suite 800
Washington, D.C. 20005
(800) 673-1290

12. A Note About Children. We do not intentionally gather Personal Data about visitors who are under the age of 13.

13. Changes to This Privacy Policy. This Privacy Policy is subject to occasional revision, and if we make any substantial changes in the way we use your Personal Data, we will notify you by prominently posting notice of the changes on the Service. Any material changes to this Privacy Policy will be effective thirty (30) calendar days following our posting of notice of the changes on our site. These changes will be effective immediately for new users of the Service. In any event, changes to this Privacy Policy may affect our use of Personal Data that you provided us prior to our notification to you of the changes. If you do not wish to permit changes in our use of your Personal Data, you must notify us prior to the effective date of the changes that you wish to deactivate your account with us. Continued use of the Service following notice of such changes shall indicate your acknowledgement of such changes and agreement to be bound by the terms and conditions of such changes.

Last Updated: August 8, 2013

Report

EXHIBIT H-2

MELANOMA RESEARCH FOUNDATION
Inspiring Hope & Progress
TWENTIETH ANNIVERSARY

Privacy Policy

Melanoma Research Foundation Privacy Policy

The Melanoma Research Foundation ("**MRF**" or "**we**," "**us**," or "**our**") is committed to protecting your privacy. We have prepared this Privacy Policy to describe to you our practices regarding the Personal Data (as defined below) we collect when you use our website as well as when you communicate with us or provide us information offline (collectively, the "**Service**").

1. User Consent. By submitting Personal Data through the Service, you agree to the terms of this Privacy Policy and you expressly consent to the processing of your Personal Data in accordance with this Privacy Policy.

2. A Note to Users Outside of the United States. Your Personal Data may be processed in the country in which it was collected and in other countries, including the United States, where laws regarding processing of Personal Data may be less stringent than the laws in your country. We adhere to the United States / European Union Data Protection Safe Harbor Arrangement, which can be located at http://www.export.gov/safeharbor/.

3. Types of Data We Collect. The MRF collects Personal Data and Anonymous Data from you when you send us information or communications and/or when you use the Service. "**Personal Data**" means data that allows someone to identify or contact you, including, for example, your name, address, telephone number, e-mail address, as well as any other non-public information about you that is associated with or linked to any of the foregoing data. "**Anonymous Data**" means data that is not associated with or linked to your Personal Data; Anonymous Data does not permit the identification of individual persons. We collect Personal Data and Anonymous Data, as described below.

3.1 Personal Data You Provide to Us. We collect Personal Data from you, such as your first and last name, e-mail and mailing addresses, and phone number, when you do any of the following:

- Donate money through the Service;
- Sign up for an online newsletter or other informational or promotional communications;
- Sign up as a volunteer or member;
- Create or modify your account on the Service;

- Provide us feedback or contact us via e-mail or the Service;
- Elect to post or submit messages, questions, comments, or other content to the Service; or
- Provide information at any point in the Service that states that Personal Data is being collected.

3.2 Personal Data Collected via Technology. To make our Service more useful to you, we collect Personal Data from you through our servers (which may be hosted by a third party service provider) and/or third party tools, including:

- Browser type, operating system, and Internet Protocol (IP) address (a number that is automatically assigned to your computer when you use the Internet, which may vary from session to session);
- Date/time stamp for your visit; and
- Cookies (as defined below) and navigational data like Uniform Resource Locators (URL) to gather information regarding the date and time of your visit and the solutions and information for which you searched and which you viewed. Like most Internet services, we automatically gather this Personal Data and store it in log files each time you visit the Service. "Cookies" are small pieces of information that a website sends to your computer's hard drive while you are viewing a web site. We may use both session Cookies (which expire once you close your web browser) and persistent Cookies (which stay on your computer until you delete them) to provide you with a more personal and interactive experience on our website. Persistent Cookies can be removed by following Internet browser help file directions. If you choose to disable Cookies, some areas of our website may not work properly.

4. Use of Your Data

4.1 General Use. In general, Personal Data you submit to us is used either to respond to requests that you make, or to aid us in serving you better. If you contact or interact with us offline and provide us with your phone number, name, street address, or email address, we will retain that information for our records, and may combine that information with information collected online or from third-party sources. We may use that information to contact you regarding events, news items, or health-related topics.The MRF uses your Personal Data in the following ways:

- Provide improved administration of the Service;
- Improve the quality of experience when you interact with the Service;
- Facilitate the creation of and secure your account on our network;
- Send you administrative e-mail notifications, such as security or support and maintenance advisories;
- Respond to your inquiries related to employment opportunities, questions about melanoma, or other requests;
- Respond to comments or messages you post on the Service;
- Thank you for your donation; and
- To send you promotional communications or our online newsletter.

4.2 Creation of Anonymous Data. We may create Anonymous Data records from Personal Data by excluding information (such as your name) that makes the data personally identifiable to you. We use this Anonymous Data to analyze request and usage patterns so that we may enhance the

content of the Service and improve site navigation. The MRF reserves the right to use and disclose Anonymous Data in its sole discretion.

4.3 Feedback. If you provide feedback to us on the Service, we may use such feedback for any purpose; provided we will not associate such feedback with your Personal Data. The MRF will collect any information contained in such communication and will treat the Personal Data in such communication in accordance with this Privacy Policy.

5. Disclosure of Your Personal Data

5.1 Affiliates. Although we currently do not have a parent company, any subsidiaries, joint ventures, or other companies under a common control (collectively, "**Affiliates**"), we may in the future. We may share some or all of your Personal Data with these Affiliates, in which case we will require our Affiliates to honor this Privacy Policy. If another company acquires our company or our assets, that company will possess the Personal Data collected by it and us and will assume the rights and obligations regarding your Personal Data as described in this Privacy Policy.

5.2 Other Disclosures. Regardless of any choices you make regarding your Personal Data (as described below), the MRF may disclose Personal Data if it believes in good faith that such disclosure is necessary to (a) comply with relevant laws or to respond to subpoenas or warrants served on the MRF; or (b) protect or defend the rights or property of the MRF or users of the Service.

6. Third parties

6.1 Personal and/or Anonymous Data Collected by Third Parties. We may receive Personal and/or Anonymous Data about you from other sources like telephone or fax, or from companies that provide services, such as, but not limited to, co-branded websites or services and online donations ("Third Party Companies"). Our Third Party Companies may supply us with Personal Data, such as your name, address, and email address. We may add this information to the information we have already collected from you via the Service to improve the Service, to send you a thank you, or to send you our online newsletter. Our provision of a link to any other website or location, such as, but not limited to, donation processing websites, is for your convenience and does not signify our endorsement of such other website or location or its contents. When you click on such a link, you will leave our site and go to another site. During this process, another entity may collect Personal Data or Anonymous Data from you. We have no control over, do not review, and cannot be responsible for, these outside websites or their content. Please be aware that the terms of this Privacy Policy do not apply to these outside websites or content, or to any collection of data after you click on links to such outside websites.

6.2 Disclosure to Third Party Service Providers and Third Party Companies. Except as otherwise stated in this policy, we do not generally sell, trade, share, or rent the Personal Data collected from our services to other entities. We will not share the information we collect from you offline with third parties, other than parties acting on our behalf, such as contractors, agents, or vendors. Unless you provide your consent, we will not share information you provide offline with parties engaged in online behavioral advertising or for purposes other than those described in this Privacy Policy. However, we may share your Personal Data with third party service providers to provide you with the Service; to conduct quality assurance testing; to facilitate creation of accounts; to provide technical support; to send you our online newsletter, to enable online

donations, or to provide other services. These third party service providers are required not to use your Personal Data other than to provide the services requested by the MRF. You expressly consent to the sharing of your Personal Data with our contractors and other service providers for the sole purpose of providing services to you. We do not sell or share your Personal Data with Third Party Companies. If you wish to have your information deleted from our records, please contact the MRF at info@melanoma.org or (800) 673-1290.

6.3 Links to Other Sites. Our Service contains links to Internet sites maintained by third parties. These links are provided for your reference only. We do not control, operate or endorse in any respect information, products, or services on such third-party sites and are not responsible for their content. Many third-party sites have their own privacy policies that differ from ours. This Privacy Policy only covers our Service and does not cover any other site.

6.4 Social Media. The MRF believes that the information contained on our social media pages might be helpful for our families and supporters. Sharing this information does not indicate an official endorsement from the MRF of the organizations from where the information was shared.

7. Donation Information. If you choose to donate to the MRF via our website, we or our third-party service provider will collect your payment information. To make any payments via the Service you will be required to give us, or our third party service providers a valid credit card number and associated payment information at the time you are required to make such payments, including all of the following: (1) your name as it appears on the card, (2) the credit card type, (3) the date of expiration of your credit card, (4) any activation numbers or codes needed to charge your card, and (5) billing address. You agree that no additional notice or consent is required before we (or our third party service providers) invoice your credit card provided to us for all amounts payable. We use our partners and third-party service providers to assist with billing and payment processes. Any Personal Data you provide to such third-party service provider will be subject to that third-party service provider's privacy policy and website terms of use, and not to this Privacy Policy or our terms of use.

8. Your Choices Regarding Your Personal Data

8.1 Choices. We offer you choices regarding the collection, use, and sharing of your Personal Data. We may periodically send you free newsletters and e-mails that directly promote the use of the Service and /or provide you information on our goals and progress. When you receive newsletters or promotional communications from us, you may indicate a preference to stop receiving further communications from us and you will have the opportunity to "opt-out" by following the unsubscribe instructions provided in the e-mail you receive or by contacting us directly (please see contact information below). Should you decide to opt-out of receiving future mailings, we may share your e-mail address with third parties to ensure that you do not receive further communications from third parties. Despite your indicated e-mail preferences, we may send you administrative e-mails regarding the Service or notices of any updates to our terms of use or Privacy Policy. You may not opt-out of these communications, which are not promotional in nature, but if you do not wish to receive these announcements, you have the option to deactivate your membership account.

8.2 Changes to Personal Data. You may change any of your Personal Data in your account by sending an e-mail to us at the e-mail address set forth below. You may request deletion of your Personal Data by us, but please note that we may be required (by law or otherwise) to keep this

information and not delete it (or to keep this information for a certain time, in which case we will comply with your deletion request only after we have fulfilled such requirements). When we delete any information, it will be deleted from the active database, but may remain in our archives.

9. Shared or Public Areas of the Service. Please be aware that if you enter any Personal Data into public or shared sections of the Service, such as, but not limited to, the chat room and bulletin board, your Personal Information will be displayed to anyone who has access to these sections of the Service. The MRF has no control over, and will have no liability to you regarding, other users' use or disclosure of such Personal Data.

10. Security of Your Personal Data. The MRF is committed to protecting the security of your Personal Data. We use a variety of industry-standard security technologies and procedures to help protect your Personal Data from unauthorized access, use, or disclosure. Despite these measures, you should know that the MRF cannot fully eliminate security risks associated with Personal Data and cannot guarantee that unauthorized access to your information will never occur.

11. Contact Information. The MRF welcomes your comments or questions regarding this Privacy Policy. Please e-mail us at info@melanoma.org or contact us at the following address or phone number:

Melanoma Research Foundation
Attn: Website Coordinator
1411 K Street NW Suite 800
Washington, D.C. 20005
(800) 673-1290

12. A Note About Children. We do not intentionally gather Personal Data about visitors who are under the age of 13.

13. Changes to This Privacy Policy. This Privacy Policy is subject to occasional revision, and if we make any substantial changes in the way we use your Personal Data, we will notify you by prominently posting notice of the changes on the Service. Any material changes to this Privacy Policy will be effective thirty (30) calendar days following our posting of notice of the changes on our site. These changes will be effective immediately for new users of the Service. In any event, changes to this Privacy Policy may affect our use of Personal Data that you provided us prior to our notification to you of the changes. If you do not wish to permit changes in our use of your Personal Data, you must notify us prior to the effective date of the changes that you wish to deactivate your account with us. Continued use of the Service following notice of such changes shall indicate your acknowledgement of such changes and agreement to be bound by the terms and conditions of such changes.

Last Updated: March 30, 2016

Report

EXHIBIT I-1

Website Privacy Notice

Our Privacy Policy

Last Revised: February 25, 2015

Thanks for visiting our website. Adventist Health System appreciates your interest in our company and health care facilities. This Privacy Policy ("Privacy Policy") outlines how we may use, maintain and protect any information that you may give us through our website.

Please also remember that your use of our website means that you have agreed to abide by all of the terms and conditions of this Privacy Policy.

Information We Receive

We receive information in different ways through our website. We reserve the right to treat anonymous or personally identifiable information collected through this website as an asset which may be transferred to a third party in connection with the merger or sale of Adventist Health System, or a portion of our business. The information we receive from users of our website can be categorized as being either anonymous or personally identifiable.

Anonymous information refers to information that cannot be tied to a specific individual. Many persons who access our website do not use the personalization features that are available to them through our website, and therefore these individuals are anonymous to us and the data we collect from them does not enable us to identify them in any personal way. For example, we may know that 5,000 users visit our website every day and that 3,000 of them reside in Florida, but we may not know their names or where they live. All anonymous information we collect through our website is collected when your web browser accesses our website. When you surf the Internet, your web browser automatically transmits information about your preferences to our server every time you visit our website. Also, our server automatically collects the IP (which stands for Internet Protocol) address of the computers that access our website. An IP address is a number that is assigned to your computer when you access the Internet. It is not truly personally identifiable information because many different individuals can access the Internet via the same computer. Please note that although such information is not personally identifiable, we can determine from an IP address a visitor's Internet Service Provider and the geographic location of his or her point of connectivity.

The anonymous information collected by us through your web browser and our server is used in aggregate form to help us to monitor audience size, measure traffic patterns and identify popular services and information within our website. We use this information to improve our services to you and to help develop improved services based on user interests, behavior and demographics.

Personally identifiable information refers to information that tells us information that can be used to identify you, such as your name, address, age, etc. In many cases, we ask for this information to provide the personalized service you wish to use. The amount of personally identifiable information that we know about you is entirely up to you to decide. We will only know personally identifiable information about you if you choose to share this information about yourself; however, some services may not be available unless we obtain a certain amount of personally identifiable information from you.

We collect personally identifiable information when you voluntarily provide it when, for example, requesting a newsletter that we produce or indicating that you would we like to receive certain targeted information on topics that interest you.

Request an Appointment
Pre-registration and Account Information
Preparing For Your Visit
Share Your Experience
What to Expect

GET STARTED

Pre-Register For An Appointment
Find A Doctor
ASK-A-NURSE
Pay Your Bill

Cookies and Web Beacons

In addition, we may also collect anonymous information through the use of "Cookies" and "Web Beacons". When you visit our website for the first time, our server sends a Cookie to your computer's hard drive through your web browser. A "Cookie" is a small text file that contains a unique identification number that is sent from us and stored on your computer. Cookies enable us to recognize your web browser whenever you visit our website through the unique identification number assigned to the Cookie, and this information is stored to help facilitate your use of the website the next time you visit. A "Web Beacon" is a small transparent image placed on a website that may track visits to a particular page. We use Web Beacons to collect information to support our reporting software.

If you wish to find out how to prevent your browser from accepting new Cookies or Web Beacons, how to disable Cookies or Web Beacons altogether and how to monitor when you receive a new Cookie or Web Beacon, check the "help" feature of your web browser. However, not accepting or disabling Cookies or Web Beacons from our websites may prevent you from accessing certain parts of our websites.

Disclosure of and Access to Information

As a general rule, we will not disclose your personally identifiable information to any unaffiliated third party, except when we have your permission or under special circumstances, such as when we need to treat the information collected through this website as an asset in the event of the merger of sale of Adventist, or a portion of our business. Your personally identifiable information may be accessed by our management information services team or an affiliated third party providing technical support or maintenance for us.

If we offer services using or in conjunction with an unaffiliated third party, we may need to share some or all of your personally identifiable information with that unaffiliated third party for purposes of providing the services to you. If you do not want your personally identifiable information to be shared, you can choose not to use that particular service or notify us that you do not wish your personally identifiable information to be shared. In some circumstances we may be required by law to disclose personally identifiable information. We will do so, in good faith, only to the extent we believe to be required by law. We may also disclose personally identifiable information in special cases when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against a third party who may be violating our terms and conditions governing the use of our website, or who may be (intentionally or unintentionally) causing injury to or interference with your or our rights or property or those of a third party.

We may share anonymous information with third parties. For example, we may match our user information, such as gender and age preferences and usage, with data of these third parties to help develop additional products and services to offer through our website.

Security Measures

Adventist Health System has taken reasonable steps and has employed industry-standard practices and technology to ensure the integrity and confidentiality of personally identifiable information; but because even the most secure computer system can be violated, Adventist Health System cannot guarantee security.

IMPORTANT: Please keep in mind that whenever you voluntarily disclose information about yourself in the public domain, for example, through bulletin boards, chat rooms, e-mails, it is likely to be collected and used by third parties. These third parties may use your information to contact you or for unauthorized purposes. Also, please remember that no one can guarantee the absolute security of information transmitted electronically.

Updating, Correcting and Deleting Personally Identifiable Information

We strongly believe in providing you with the ability to opt-out of providing personally identifiable to us, and to access and edit any information you may have provided to us about yourself. Accordingly, at any time, you may amend, update or delete the information about you (or your child(ren)) contained in any registration profile you have completed with us, including any and all personally identifiable information, or stop receipt of a newsletter, by mailing your request to:

Adventist Health System
900 Hope Way
Altamonte Springs, Florida 32714
Attn: Data Security

Links

Our website may contain links to other sites. These links are for your convenience only, and Adventist Health System makes no representations or endorsements whatsoever regarding such other sites. You should review the privacy policies of other sites carefully before providing any information to such website. Adventist Health System is not responsible for the privacy policies or procedures or the content of any other website.

Changes to Privacy Policy

Adventist Health System may modify or change this Privacy Policy at any time. Such modifications or changes become effective immediately when

they are posted to this website. You agree to review this Privacy Policy frequently so that you will be familiar with the terms. You further agree that each time you use this website that you are, by such use, consenting to the terms of this Privacy Policy that are applicable at your time of use.

Children

We are committed to protecting children's privacy on the Internet and we do not knowingly collect personal information from children.

Adventist Health System's Limited Warranties; Disclaimer of Liability; Indemnity by You

ADVENTIST HEALTH SYSTEM DOES NOT MAKE ANY EXPRESS OR IMPLIED WARRANTIES, REPRESENTATIONS OR ENDORSEMENTS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE OR NONINFRINGEMENT, OR THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) REGARDING INFORMATION, CONTENT OR ITEMS APPEARING ON THIS WEBSITE. ADVENTIST HEALTH SYSTEM DOES NOT WARRANT THAT DOWNLOADS FROM THE WEBSITE WILL BE FREE OF ANY VIRUS, WORM, TROJAN HORSE OR OTHER DATA ALTERING OR CONTAMINATING COMPONENTS. YOU ARE RESPONSIBLE FOR ENSURING THAT YOU HAVE IMPLEMENTED PROCEDURES TO PREVENT SUCH CONTAMINATING COMPONENTS FROM INFECTING YOUR COMPUTER AND ITS DATA.

WHILE ADVENTIST HEALTH SYSTEM TRIES TO KEEP THE INFORMATION ON THIS WEBSITE BOTH ACCURATE AND UP-TO-DATE, ADVENTIST HEALTH SYSTEM DOES NOT WARRANT THE ACCURACY, COMPLETENESS, CORRECTNESS, USEFULNESS, OR APPLICABILITY OF ANY INFORMATION, OR OTHER DATA OR ITEMS APPEARING ON THIS WEBSITE. ADVENTIST HEALTH SYSTEM WILL NOT BE LIABLE IN ANY EVENT TO ANY USER OF THIS SERVICE FOR ANY DECISION MADE OR ACTION TAKEN IN RELIANCE UPON THE INFORMATION, CONTENT, OR OTHER ITEMS PRESENTED ON THIS WEBSITE.

IN NO EVENT SHALL ADVENTIST HEALTH SYSTEM BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE, OR ANY OTHER MONETARY OR OTHER DAMAGES, FEES, FINES, PENALTIES, OR LIABILITIES ARISING OUT OF OR RELATING IN ANY WAY TO THIS WEBSITE, OR WEBSITES ACCESSED THROUGH THIS WEBSITE, AND/OR THEIR CONTENT OR INFORMATION. A USER'S SOLE AND EXCLUSIVE REMEDY FOR DISSATISFACTION WITH THE WEBSITE IS TO STOP USING THE WEBSITE.

ADVENTIST HEALTH SYSTEM DOES NOT GUARANTEE CONTINUOUS OR UNINTERRUPTED ACCESS TO THIS WEBSITE, AND OPERATION OF THIS WEBSITE MAY BE INTERFERED WITH BY FACTORS BEYOND ADVENTIST

HEALTH SYSTEM'S CONTROL. YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD ADVENTIST HEALTH SYSTEM HARMLESS, AS WELL AS ADVENTIST HEALTH SYSTEM'S OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, INFORMATION PROVIDERS AND SUPPLIERS FROM AND AGAINST ALL LOSSES, EXPENSES, DAMAGES AND COSTS, INCLUDING REASONABLE ATTORNEY'S FEES, RESULTING FROM YOUR VIOLATION OF THESE CONDITIONS OF USE OR THE USE OF THIS SERVICE.

Use of This Website Creates an Agreement

Your continued use of this website constitutes your agreement to this Privacy Policy. This Privacy Policy forms an agreement that is entered into and is subject to the laws of the State of Florida. Those laws will apply, except the choice of law statutes, in construing and interpreting this agreement. If any provision of this agreement is held to be unenforceable, invalid, void or voidable, by a court or other tribunal of competent jurisdiction, then such provision shall be given a limited effect or shall be eliminated to the extent necessary so that the remaining provisions of this agreement remain in full force and effect.

Prohibited Use of This Website

If you live in a state or country that has laws that would either (1) void or alter these terms and conditions or (2) make illegal the access or use of this website, then your use of this website is unauthorized; it cannot be sanctioned by Adventist Health System, and you use the website at your own risk.

Disclaimer

This Privacy Policy only applies to information collected through this website. This Privacy Policy does not apply to personally identifiable information received or created by Adventist Health System from any of the following Adventist Health System Services:

Online search and application for employment opportunities at Adventist Health System, other than physician career opportunities. These employment search activities are provided by a third-party website operator and subject to a separate privacy policy. If you wish to review the privacy policy which applies to online employment search and application, please see this webpage http://www.adventisthealthsystem.com/page.php?section=legal&page=privacy_policy_jobs.

FHHS Member Services. If you wish to review the privacy policy which applies to FHHS Member Services, please see this webpage https://www.tpabenefits.com/web29118/privacy.asp.

Patient Care Services. Information you provide to an Adventist Health

System health care facility while being treated as a patient of that health care facility is defined as "protected health information" under the Health Insurance Portability & Accountability Act and its attendant regulations ("HIPAA") and is subject to the HIPAA Notice of Privacy Practices of that health care
facility http://www.shawneemission.org/resources/patients/patient-privacy-notice

Contacting Us Regarding this Policy or the Website

If you have questions about this Privacy Policy or any other questions concerning the website, please contact:

Data Security
Adventist Health System
900 Hope Way
Altamonte Springs, FL 32714
407-357-1000

SHAWNEE MISSION HEALTH LOCATIONS

Shawnee Mission Medical Center

Prairie Star 23401 Prairie

CONNECT WITH US

9100 West 74th Street Shawnee Mission, Kansas 66204 Get Directions

Main Number 913-676-2000

Star Parkway Lenexa, Kansas 66227 Get Directions

Main Number 913-676-8500

Register
Login

EXHIBIT I-2

Website Privacy Notice

Our Privacy Policy

Last Revised: February 25, 2015

Thanks for visiting our website. Adventist Health System appreciates your interest in our company and health care facilities. This Privacy Policy ("Privacy Policy") outlines how we may use, maintain and protect any information that you may give us through our website.

Please also remember that your use of our website means that you have agreed to abide by all of the terms and conditions of this Privacy Policy.

Information We Receive

Resources
Patients

Advance Directive
Estimate Your Out-of Pocket Cost
Financial Assistance
Finar
Medi
Mino
Patie
Patie
Patie
Pay Y
Prepa
Share
What
Webs

3 Trackers
Google Analytics
Google Tag Ma...
Visual Website ...

We receive information in different ways through our website. We reserve the right to treat anonymous or personally identifiable information collected through this website as an asset which may be transferred to a third party in connection with the merger or sale of Adventist Health System, or a portion of our business. The information we receive from users of our website can be categorized as being either anonymous or personally identifiable.

Anonymous information refers to information that cannot be tied to a specific individual. Many persons who access our website do not use the personalization features that are available to them through our website, and therefore these individuals are anonymous to us and the data we collect from them does not enable us to identify them in any personal way. For example, we may know that 5,000 users visit our website every day and that 3,000 of them reside in Florida, but we may not know their names or where they live. All anonymous information we collect through our website is collected when your web browser accesses our website. When you surf the Internet, your web browser automatically transmits information about your preferences to our server every time you visit our website. Also, our server automatically collects the IP (which stands for Internet Protocol) address of the computers that access our website. An IP address is a number that is assigned to your computer when you access the Internet. It is not truly personally identifiable information because many different individuals can access the Internet via the same computer. Please note that although such information is not personally identifiable, we can determine from an IP address a visitor's Internet Service Provider and the geographic location of his or her point of connectivity.

The anonymous information collected by us through your web browser and our server is used in aggregate form to help us to monitor audience size, measure traffic patterns and identify popular services and information within our website. We use this information to improve our services to you and to help develop improved services based on user interests, behavior and demographics.

Personally identifiable information refers to information that tells us information that can be used to identify you, such as your name, address, age, etc. In many cases, we ask for this information to provide the personalized service you wish to use. The amount of personally

identifiable information that we know about you is entirely up to you to decide. We will only know personally identifiable information about you if you choose to share this information about yourself; however, some services may not be available unless we obtain a certain amount of personally identifiable information from you.

We collect personally identifiable information when you voluntarily provide it when, for example, requesting a newsletter that we produce or indicating that you would we like to receive certain targeted information on topics that interest you.

Cookies and Web Beacons

In addition, we may also collect anonymous information through the use of "Cookies" and “Web Beacons”. When you visit our website for the first time, our server sends a Cookie to your computer's hard drive through your web browser. A “Cookie” is a small text file that contains a unique identification number that is sent from us and stored on your computer. Cookies enable us to recognize your web browser whenever you visit our website through the unique identification number assigned to the Cookie, and this information is stored to help facilitate your use of the website the next time you visit. A "Web Beacon" is a small transparent image placed on a website that may track visits to a particular page. We use Web Beacons to collect information to support our reporting software.

If you wish to find out how to prevent your browser from accepting new Cookies or Web Beacons, how to disable Cookies or Web Beacons altogether and how to monitor when you receive a new Cookie or Web Beacon, check the "help" feature of your web browser. However, not accepting or disabling Cookies or Web Beacons from our websites may prevent you from accessing certain parts of our websites.

Disclosure of and Access to Information

As a general rule, we will not disclose your personally identifiable information to any unaffiliated third party, except when we have your permission or under special circumstances, such as when we need to treat the information collected through this website as an asset in the event of the merger of sale of Adventist, or a portion of our business. Your personally identifiable information may be accessed by our

management information services team or an affiliated third party providing technical support or maintenance for us.

If we offer services using or in conjunction with an unaffiliated third party, we may need to share some or all of your personally identifiable information with that unaffiliated third party for purposes of providing the services to you. If you do not want your personally identifiable information to be shared, you can choose not to use that particular service or notify us that you do not wish your personally identifiable information to be shared. In some circumstances we may be required by law to disclose personally identifiable information. We will do so, in good faith, only to the extent we believe to be required by law. We may also disclose personally identifiable information in special cases when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against a third party who may be violating our terms and conditions governing the use of our website, or who may be (intentionally or unintentionally) causing injury to or interference with your or our rights or property or those of a third party.

We may share anonymous information with third parties. For example, we may match our user information, such as gender and age preferences and usage, with data of these third parties to help develop additional products and services to offer through our website.

Security Measures

Adventist Health System has taken reasonable steps and has employed industry-standard practices and technology to ensure the integrity and confidentiality of personally identifiable information; but because even the most secure computer system can be violated, Adventist Health System cannot guarantee security.

IMPORTANT: Please keep in mind that whenever you voluntarily disclose information about yourself in the public domain, for example, through bulletin boards, chat rooms, e-mails, it is likely to be collected and used by third parties. These third parties may use your information to contact you or for unauthorized purposes. Also, please remember that no one can guarantee the absolute security of information transmitted electronically.

Updating, Correcting and Deleting Personally Identifiable Information

We strongly believe in providing you with the ability to opt-out of providing personally identifiable to us, and to access and edit any information you may have provided to us about yourself. Accordingly, at any time, you may amend, update or delete the information about you (or your child(ren)) contained in any registration profile you have completed with us, including any and all personally identifiable information, or stop receipt of a newsletter, by mailing your request to:

Adventist Health System
900 Hope Way
Altamonte Springs, Florida 32714
Attn: Data Security

Links

Our website may contain links to other sites. These links are for your convenience only, and Adventist Health System makes no representations or endorsements whatsoever regarding such other sites. You should review the privacy policies of other sites carefully before providing any information to such website. Adventist Health System is not responsible for the privacy policies or procedures or the content of any other website.

Changes to Privacy Policy

Adventist Health System may modify or change this Privacy Policy at any time. Such modifications or changes become effective immediately when they are posted to this website. You agree to review this Privacy Policy frequently so that you will be familiar with the terms. You further agree that each time you use this website that you are, by such use, consenting to the terms of this Privacy Policy that are applicable at your time of use.

Children

We are committed to protecting children's privacy on the Internet and we do not knowingly collect personal information from children.

Adventist Health System's Limited Warranties; Disclaimer of Liability; Indemnity by You

ADVENTIST HEALTH SYSTEM DOES NOT MAKE ANY EXPRESS OR IMPLIED WARRANTIES, REPRESENTATIONS OR ENDORSEMENTS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE OR NONINFRINGEMENT, OR THE IMPLIED WARRANTIES OF

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) REGARDING INFORMATION, CONTENT OR ITEMS APPEARING ON THIS WEBSITE. ADVENTIST HEALTH SYSTEM DOES NOT WARRANT THAT DOWNLOADS FROM THE WEBSITE WILL BE FREE OF ANY VIRUS, WORM, TROJAN HORSE OR OTHER DATA ALTERING OR CONTAMINATING COMPONENTS. YOU ARE RESPONSIBLE FOR ENSURING THAT YOU HAVE IMPLEMENTED PROCEDURES TO PREVENT SUCH CONTAMINATING COMPONENTS FROM INFECTING YOUR COMPUTER AND ITS DATA.

WHILE ADVENTIST HEALTH SYSTEM TRIES TO KEEP THE INFORMATION ON THIS WEBSITE BOTH ACCURATE AND UP-TO-DATE, ADVENTIST HEALTH SYSTEM DOES NOT WARRANT THE ACCURACY, COMPLETENESS, CORRECTNESS, USEFULNESS, OR APPLICABILITY OF ANY INFORMATION, OR OTHER DATA OR ITEMS APPEARING ON THIS WEBSITE. ADVENTIST HEALTH SYSTEM WILL NOT BE LIABLE IN ANY EVENT TO ANY USER OF THIS SERVICE FOR ANY DECISION MADE OR ACTION TAKEN IN RELIANCE UPON THE INFORMATION, CONTENT, OR OTHER ITEMS PRESENTED ON THIS WEBSITE.

IN NO EVENT SHALL ADVENTIST HEALTH SYSTEM BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE, OR ANY OTHER MONETARY OR OTHER DAMAGES, FEES, FINES, PENALTIES, OR LIABILITIES ARISING OUT OF OR RELATING IN ANY WAY TO THIS WEBSITE, OR WEBSITES ACCESSED THROUGH THIS WEBSITE, AND/OR THEIR CONTENT OR INFORMATION. A USER'S SOLE AND EXCLUSIVE REMEDY FOR DISSATISFACTION WITH THE WEBSITE IS TO STOP USING THE WEBSITE.

ADVENTIST HEALTH SYSTEM DOES NOT GUARANTEE CONTINUOUS OR UNINTERRUPTED ACCESS TO THIS WEBSITE, AND OPERATION OF THIS WEBSITE MAY BE INTERFERED WITH BY FACTORS BEYOND ADVENTIST HEALTH SYSTEM'S CONTROL. YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD ADVENTIST HEALTH SYSTEM HARMLESS, AS WELL AS ADVENTIST HEALTH SYSTEM'S OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, INFORMATION PROVIDERS AND SUPPLIERS FROM AND AGAINST ALL LOSSES, EXPENSES, DAMAGES AND COSTS, INCLUDING REASONABLE ATTORNEY'S FEES, RESULTING FROM YOUR VIOLATION OF THESE CONDITIONS OF USE OR THE USE OF THIS SERVICE.

Use of This Website Creates an Agreement

Your continued use of this website constitutes your agreement to this Privacy Policy. This Privacy Policy forms an agreement that is entered into and is subject to the laws of the State of Florida. Those laws will apply, except the choice of law statutes, in construing and interpreting this agreement. If any provision of this agreement is held to be unenforceable, invalid, void or voidable, by a court or other tribunal of competent jurisdiction, then such provision shall be given a limited effect or shall be eliminated to the extent necessary so that the remaining provisions of this agreement remain in full force and effect.

Prohibited Use of This Website

If you live in a state or country that has laws that would either (1) void or alter these terms and conditions or (2) make illegal the access or use of this website, then your use of this website is unauthorized; it cannot be sanctioned by Adventist Health System, and you use the website at your own risk.

Disclaimer

This Privacy Policy only applies to information collected through this website. This Privacy Policy does not apply to personally identifiable information received or created by Adventist Health System from any of the following Adventist Health System Services:

Online search and application for employment opportunities at Adventist Health System, other than physician career opportunities. These employment search activities are provided by a third-party website operator and subject to a separate privacy policy. If you wish to review the privacy policy which applies to online employment search and application, please see this webpage http://www.adventisthealthsystem.com/page.php?section=legal&page=privacy_policy_jobs.

FHHS Member Services. If you wish to review the privacy policy which applies to FHHS Member Services, please see this webpage https://www.tpabenefits.com/web29118/privacy.asp.

Patient Care Services. Information you provide to an Adventist Health System health care facility while being treated as a patient of that health care facility is defined as “protected health information” under the Health Insurance Portability & Accountability Act and its attendant regulations (“HIPAA”) and is subject to the HIPAA Notice of Privacy Practices of that

health care facility http://www.shawneemission.org/resources/patients/patient-privacy-notice

Contacting Us Regarding this Policy or the Website

If you have questions about this Privacy Policy or any other questions concerning the website, please contact:

Data Security
Adventist Health System
900 Hope Way
Altamonte Springs, FL 32714
407-357-1000

SHAWNEE MISSION HEALTH LOCATIONS

Shawnee Mission Medical Center 9100 West 74th Street Shawnee Mission,	Prairie Star 23401 Prairie Star Parkway Lenexa, Kansas 66227 Get

Connect with us:

Kansas
66204

Get
Directions

Directions

Main
Number
913-676-
8500

Main
Number
913-676-
2000

Register
Login

EXHIBIT J-1

Barnes-Jewish Hospital, Washington University School of Medicine, St. Louis Children's Hospital

BJC HealthCare | 4444 Forest Park Avenue | St. Louis, Missouri 63108 USA | phone -- 314.747.WEBB

JOINT NOTICE OF PRIVACY PRACTICES

Effective Date: April 2003
Last Revision Date: July 2015
Effective Date Following Revision: November 5, 2015

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice serves as a joint notice for Barnes-Jewish Hospital, St. Louis Children's Hospital and Washington University School of Medicine (collectively referred to herein as "we" or "our" or "us"). Because we are affiliated health care providers, we have designated ourselves as an organized health care arrangement under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. We will follow the terms of this Notice and may share health information with each other for purposes of treatment, payment and health care operations as described in this Notice. Since we maintain health information separately, we will respond separately to your questions, requests and complaints concerning your health information.

OUR DUTIES REGARDING YOUR HEALTH INFORMATION

We are required by law to protect the privacy of your protected health information, to provide you with notice of these legal duties and to notify you following a breach of unsecured protected health information. This Notice explains how, when and why we typically use and disclose health information and your privacy rights regarding your health information. In our Notice, we refer to our uses and disclosures of health information as our "Privacy Practices." Protected health information generally includes information that we create or receive that identifies you and your past, present or future health status or care, or the provision of or payment for that health care. We are obligated to abide by these Privacy Practices as of the effective dates listed below.

WHO WILL FOLLOW THIS NOTICE

Our Notice serves as a Joint Notice and we will follow the terms of this Notice. This Notice, however, also describes the Privacy Practices of BJC HealthCare and its wholly owned subsidiaries and affiliated facilities described in the attached list and personnel ("BJC affiliated sites"), the Privacy Practices of Washington University School of Medicine and its wholly owned subsidiaries and affiliated facilities described in the attached list and their respective personnel, including Washington University Clinical Associates, L.L.C. and its wholly owned subsidiaries, affiliated practices and their respective personnel ("WUCA").

Specifically, our Notice also describes the Privacy Practices of:

- Any BJC HealthCare affiliated hospital or service, all departments and units of our affiliated hospitals, and the health care professionals and other BJC HealthCare affiliated hospital personnel, including those employees or personnel of any other BJC HealthCare affiliated sites
- All Washington University School of Medicine health care providers, their staff and affiliated practices
- Any member of a volunteer group we allow to help you while you are receiving care from us

CHANGES TO THIS NOTICE

We reserve the right to change our Privacy Practices and the terms of this Notice. We will provide you with any revised Notice by making it available to you upon request and by posting it at our service sites. We will also post the revised Notice on our websites. Any changes that we make in our Privacy Practices will affect any protected health information that we maintain.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU WITHOUT YOUR WRITTEN CONSENT OR AUTHORIZATION

For Treatment, Payment and Health Care Operations

1. **For Your Treatment.** We may use and/or disclose your health information to health care providers and other personnel who are involved in your care and who will provide you with medical treatment or services. For example, if you have had surgery or just had a baby, we may contact a home health care agency to arrange for home services or to check on your recovery after you are discharged from the hospital.

2. **For Payment of Health Services.** We may use and/or disclose your health information to bill and receive payment for the services that you receive from us. For example, we may provide your health information to our billing or claims department to prepare a bill or statement to send to you, your insurance company, including Medicare or Medicaid, or another group or individual that may be responsible to pay for your health services.

3. **For Our Health Care Operations.** We may use or disclose your health information to carry out certain administrative, financial, legal and quality improvement activities that are

necessary to run our businesses and to support our treatment and payment activities. For example, we may use and/or disclose your health information to help assess the quality and performance of our physicians and staff and improve the services that we provide. Specifically, we may disclose your health information to physicians, medical or other health or business professionals for review, consultation, comparison and planning. We may use and disclose your health information in the course of our training programs and for accreditation, certification, licensing or credentialing activities. Additionally, we may disclose your health information to auditors, accountants, attorneys, government regulators or other consultants to assess and/or ensure our compliance with laws or to represent us before regulatory or other governing authorities or judicial bodies.

4. **Special Circumstances When We May Disclose Your Health Information on a Limited Basis.** After removing direct identifying information (such as your name, address and Social Security number), we may use your health information for research, public health activities and other health care operations (such as business planning). While only limited identifying information will be used, we will also obtain assurances from the recipient of such health information that they will safeguard the information and only use and disclose the information for limited purposes.

In conducting or participating in activities related to treatment, payment and health care operations, we may add or combine your information into electronic (computer) databases with information from other health care providers to help us improve our health services. For instance, using a combined information database, we may have more information to help us make more informed decisions about the range of treatments and care that may be available to you, including avoiding duplicate tests or conflicting treatment decisions. While we may not notify you about the inclusion of your data into these databases, you may be permitted to "opt-out" of some of these databases. We will make reasonable attempts to notify our patients, and perhaps the general public, of such opt-out options (when available) by posting notices in our facilities, on our websites or through social media.

For Activities Permitted or Required by Law

There are situations where we may use and/or disclose your health information without first obtaining your written authorization for purposes other than for treatment, payment or health care operations. Except for the specific situations where the law requires us to use and disclose information (such as reports of births to the health department or reports of abuse or neglect to

social services), we have listed all these permitted uses and disclosures in this section.

1. **Public Health Activities.** We may disclose your health information to a public health authority that is authorized by law to collect or receive information in order to report, among other things, communicable diseases and child abuse, or to the U.S. Food and Drug Administration (FDA) to report medical device or product-related events. In certain limited situations, we may also disclose your health information to notify a person exposed to a communicable disease.

2. **Health Oversight Activities.** We may disclose your health information to a health oversight agency that includes, among others, an agency of the federal or state government that is authorized by law to monitor the health care system.

3. **Law Enforcement Activities.** We may disclose your health information in response to a law enforcement official's request for information to identify or locate a victim, a suspect, a fugitive, a material witness or a missing person (including individuals who have died) or for reporting a crime that has occurred on our premises or that may have caused a need for emergency services.

4. **Judicial and Administrative Proceedings.** We may disclose your health information in response to a subpoena or order of a court or administrative tribunal.

5. **Coroners, Medical Examiners and Funeral Directors.** We may disclose your health information to coroners, medical examiners and funeral directors to identify a deceased person or to determine the cause of death.

6. **Organ Donation.** We may disclose your health information to an organ procurement organization or other facility that participates in or makes a determination for the procurement, banking and/or transplantation of organs or tissues.

7. **Research Purposes.** We conduct and participate in medical, social, psychological and other types of research. Most human subject research projects, including many of those involving the use of health information, are subject to a special approval process which evaluates the proposed research project and its use of health information. In certain circumstances, however, we may disclose health information to researchers preparing to conduct a research project to help them determine whether a research project can be carried out or will be useful, so long as the health information they review does not leave our premises.

Our clinicians may offer you the opportunity to participate in a clinical research trial (investigational treatments) and other researchers may contact you regarding your interest in participating in research projects. Your enrollment in a research project will occur only after you have been informed about the research, had an opportunity to ask questions and have signed a consent form. When approved through a special review process, research may be performed using your health information without your consent.

8. **Avoidance of Harm to a Person or Public Safety.** We may disclose if we believe that the disclosure is necessary to prevent or lessen a serious threat or harm to the public or the health or safety of another person.

9. **Specialized Government Functions.** We may disclose for specific governmental security needs, or as needed by correctional institutions.

10. **Workers' Compensation Purposes.** We may disclose to comply with workers' compensation laws or similar programs.

11. **Appointment Reminders and to Inform You of Health Related Products or Services.** We may use or disclose your health information to contact you for medical appointments or other scheduled services, or to provide you with information about treatment alternatives or other health-related benefits and services.

12. **Billing and Collection Purposes.** We may use or disclose your health information for the purpose of obtaining payment for services provided. You may be contacted by mail or telephone at any telephone number associated with you, including wireless numbers. Telephone calls may be made using pre-recorded or artificial voice messages and/or automatic dialing device (an "autodialer"). Messages may be left on answering machines or voicemail, including any such message information required by law (including debt collection laws) and/or regarding amounts owed by you. Text messages or emails using any email addresses you provide may also be used in order to contact you.

13. **Fundraising Purposes.** We may use or disclose demographic information, including names, addresses, other contact information, age, gender and date of birth; the dates that you received health care from us; department of service information; treating physician information; and outcome

information to contact you in order to raise funds so that we may continue or expand our health care activities. You have the right to opt out of these fundraising activities. If you do not wish to be contacted as part of our fundraising efforts, please contact the individual(s) listed in the Contact Section of this Notice. If you decide you do not wish to be contacted as part of our fundraising efforts, we will not condition service or payment upon that decision.

When your preferences will guide our use or disclosure

1. A facility directory may include your name, your location in the facility, your general condition such as fair, stable, etc., and your religious affiliation (if provided by you). Unless you tell us that you would like to restrict your information in a facility directory, you will be included and directory information may be disclosed to members of the clergy or to people who ask for you by name.
2. We may disclose your health information to a family member, other relative, friend or any other person you identify who is involved in your care or involved with the payment related to your care unless you tell us otherwise.

Uses and Disclosures that Require Your Prior Written Authorization

1. We will not disclose psychotherapy notes without your written authorization unless the use and disclosure is otherwise permitted or required by law.
2. We will not engage in disclosures that constitute a sale of your health information without your written authorization. A sale of protected health information occurs when we, or someone we contract with directly or indirectly, receive payment in exchange for your protected health information.
3. We will not use or disclose your protected health information for marketing purposes without your written authorization. Marketing is defined as receipt of payment from a third party for communicating with you about a product or service marketed by the third party.

For situations not generally described in our Notice, we will ask for your written authorization before we use or disclose your health information. You may revoke that authorization, in writing, at any time to stop future disclosures of your health information. Information previously disclosed, however, will not be requested to be returned nor will your revocation affect any action that we have already taken in reliance on your authorization. In addition, if we collected the information in connection with a research study, we are permitted to use and disclose that information to the extent it is necessary to protect the integrity of the research study.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

Requesting Restrictions of Certain Uses and Disclosures of Health Information

You may request, in writing, a restriction on how we use or disclose your protected health information for your treatment, for payment of your health care services, or for activities related to our health care operations. You may also request a restriction on what health information we may disclose to someone who is involved in your care, such as a family member or friend. To make a request, see contact information below.

We are not required to agree to your request in all circumstances. Additionally, any restriction that we may approve will not affect any use or disclosure that we are required or permitted to make under the law. We must agree to your request to restrict disclosure of your health information to your health plan if the disclosure is not required by law and the health information you want restricted pertains solely to a health care item or service for which you (or someone other than your health plan, on your behalf) have paid us for in full.

Requesting Confidential Communications

You may request changes in the manner in which we communicate with you or the location where we may contact you. You must make your request in writing. See contact information below. We will accommodate your reasonable request, but in determining whether your request is reasonable, we may consider the administrative difficulty it may impose on us.

Inspecting and Obtaining Copies of Your Health Information

You may ask to look at and obtain a copy of your health information. You must make your request in writing. See contact information at the end of this notice.

We may charge a fee for copying or preparing a summary of requested health information. We will respond to your request for health information within 30 days of receiving your request by either providing the information requested, denying the request with a written explanation for the denial, or advising you we need additional time to complete our action on your request (for instance, if your health information is not readily accessible or the information is maintained in an off-site storage location).

Requesting a Change in Your Health Information

You may request, in writing, a change or addition to your health information. See contact information below. The law limits your ability to change or add to your health information. These limitations include whether we created or include the health information within our medical records or if we believe that the health information is accurate and complete without any changes. Under no circumstances will we erase or otherwise delete original documentation in your health information.

Requesting an Accounting of Disclosures of Your Health Information

You may ask, in writing, for an accounting of certain types of disclosures of your health information. The law excludes from an accounting many of the typical disclosures, such as those made to care for you, to pay for your health services, or where you provided your written authorization to the disclosure.

To make a request for an accounting see contact information below. Generally, we will respond to your request within 60 days of receiving your request unless we need additional time.

Notification Following a Breach of Unsecured Protected Health Information

We will notify you within a reasonable time not to exceed 60 days, in writing, in the event your health information is compromised by BJC HealthCare, Washington University School of Medicine, one of our affiliates or by someone with whom we contracted to conduct business on our behalf.

Obtaining a Notice of Our Privacy Practices

We provide you with our Notice to explain and inform you of our Privacy Practices. You may also take a copy of this Notice with you. Even if you have requested this Notice electronically, you
may request a paper copy at any time. You may also view or obtain a copy of this Notice at our websites: BJC HealthCare and Washington University School of Medicine.

COMPLAINTS

We welcome an opportunity to address any concerns that you may have regarding the privacy of your health information. If you believe that the privacy of your health information has been violated, you may file a complaint with the individuals listed in the Contact Section of this Notice. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services.

You will not be penalized or retaliated against for filing a complaint.

CONTACT INFORMATION

It is important to note that requests to Barnes-Jewish Hospital, St. Louis Children's Hospital and Washington University must be made separately. Any requests or complaints to one provider will not be deemed to be filed with any of the other providers covered by or addressed in this Joint Notice.

For questions, concerns, requests or complaints concerning Barnes-Jewish Hospital or St. Louis Children's Hospital, please contact the Barnes- Jewish Hospital operator at (314) 362-5000 or St. Louis Children's Hospital operator at (314) 454-6000 and request the Patient Liaison/Advocate or write to the Patient Liaison/Advocate at the address shown below.

For questions, concerns, requests or complaints concerning Washington University or its providers, you may contact the Privacy Officer at the telephone number or address listed below. To look at or obtain a copy or your health information from a Washington University physician or provider, you may contact the Washington University Health Information Release Service at (314) 273-0453.

Barnes-Jewish Hospital
Patient Liaison
Address: Office of Patient & Family Affairs
Attention: Patient Liaison
Mail Stop: 90-72-432
One Barnes-Jewish Hospital Plaza
St. Louis, Missouri 63110 USA
Telephone Number: (314) 362-6100

St. Louis Children's Hospital
Patient Liaison
Address: Attn: Patient Advocacy Coordinator

One Children's Place, Suite 4S50
St. Louis, Missouri 63110 USA
Telephone Number: (314) 286-0711

Washington University
Privacy Officer
Address: Campus Box 8098
660 South Euclid Avenue
St. Louis, Missouri 63110 USA
Telephone Number: toll-free (866) 747-4975

BJC HEALTHCARE SERVICE DELIVERY SITES

BJC HealthCare Hospitals

Alton Memorial Hospital
Barnes-Jewish Hospital
Barnes-Jewish St. Peters Hospital
Barnes-Jewish West County Hospital
Boone Hospital Center
Christian Hospital and Northwest HealthCare
Missouri Baptist Medical Center
Missouri Baptist Sullivan
Parkland Health Center - Bonne Terre
Parkland Health Center - Farmington
Parkland Health Center - Weber Road
Progress West Hospital
St. Louis Children's Hospital

BJC HealthCare Long-Term Care Facilities

Barnes-Jewish Extended Care
Eunice Smith Nursing Home

BJC HEALTH SERVICES

BJC Behavioral Health
BJC Corporate Health Services
BJC Home Care Services and Boone Hospital Home Care and Hospice
BJC Medical Group Offices
BJC Retail Pharmacies
BJC Vision Centers
Fairview Heights Medical Group
Heart Care Institute
Siteman Cancer Center

For more information concerning BJC HealthCare facility locations, please visit our website at www.bjc.org or call (314) 362-9355 or 1-800-392-0936.

WASHINGTON UNIVERSITY CLINICAL ASSOCIATES SERVICE DELIVERY SITES

Blue Fish Pediatrics
Cloverleaf Pediatrics
Forest Park Pediatrics
Grant Medical Group
Maryland Medical Group
Northwest Pediatrics
O'Fallon Pediatrics
University Internal Medicine and Diabetes Associates
WUCA Child Neurology Associates

LARGE PRINT

Large Print HIPAA pdf

AUDIO FILE

Audio File

TRANSLATIONS

American Sign Language

Please click on the links below to view .pdf files of this content in multiple languages:

- Arabic
- Bosnian
- Farsi
- German
- Nepali
- Russian
- Spanish
- Chinese (Simplified)
- Vietnamese

BARNES-JEWISH Hospital | Washington University in St. Louis Physicians

NATIONAL LEADERS IN MEDICINE

Terms of Use and Privacy Statement

Terms of Use

Barnes-Jewish Hospital or the "Site Sponsor"), is providing information and services on this Internet site as a benefit to our users. The information and services on this site are provided solely for general illustration, educational and resource provision purposes. Such information and services are not intended to be specific medical, health, business or other professional advice or direction. If you have specific questions regarding your health or health status, contact your physician or other health care provider. Neither the Site Sponsor nor its information contributors make any express or implied representations or warranties about the completeness or accuracy of this information and these services for any purpose or the suitability of this information or these services for any particular use.

This site will also enable users to obtain information on the services, events and materials offered, happening or available through the Site Sponsor, including publications and educational programs, current news, certain Barnes-Jewish Hospital, BJC HealthCare and Washington University School of Medicine documents, press releases, lists of health related web sites, and other information relevant to purposes of this site.

This internet site may include "links" providing direct access to other Internet sites. However, the Site Sponsor takes no responsibility for the content or information contained on those other sites, and does not exert any editorial, monitoring or other control over those other sites and therefore do not assume any liability for those sites or their content. The Site Sponsor reserves the right to remove any link from this site for any or no reason. The existence of any particular link is simply intended to imply potential interest to users of this site.

Certain areas of the site may allow for the posting or exchange of information among and between users. Users that submit or post information to this site grant the Site Sponsor the authority and right to use any submission in any way, and by such submissions warrant and represent to the Site Sponsor that such submissions are not in violation of United States copyright or other laws. In addition, the Site Sponsor reserves the right to review, edit or delete any posting or information (including, without limitation, those that appear to be inappropriate for the intended purposes of this site). Note: Any information that you include in your posting will be posted to the bulletin board and be available to any or all users, including without limitation, personal, health and demographic information.

All images, text, and other materials posted on this site are subject to copyrights owned by the Site Sponsor or other individuals or entities and are protected by United States copyright laws. Any reproduction, retransmission, distribution or republication of all or part of any images, text programs, and other materials found on this site is expressly prohibited, unless the Site Sponsor or the copyright owner of the material has expressly granted its prior written consent.

Privacy Statement

Barnes-Jewish Hospital has created this statement to demonstrate our commitment to your privacy. This statement explains our information-gathering and dissemination practices for this Web site.

A typical visit to our Web site does not require a user to submit personal information. However, if you decide to send us an e-mail, respond to a survey, or subscribe to an online publication with your contact information, we will respond to you with the information you request and other information that we think might be of interest to you. If you choose to receive more information, your name and contact information (including e-mail address) will be added to our database. From that database, we may send you materials such as newsletters, brochures or articles of interest via regular mail, e-mail or in other ways.

Information you submit may be routinely shared with our parent organization, BJC HealthCare as they often distribute our materials, or with the Washington University School of Medicine if you are looking for a physician referral. Other than these two organizations, we will only forward your personal information to organizations working on our behalf. We urge you not to provide any confidential information about you or your health to us via electronic communication. If you do so, it is at your own risk. Although we attempt to maintain or computer network in a secure manner to protect the content of your messages, we cannot provide absolute assurance that the contents of your e-mail will not become accessible to individuals or entities that are not authorized to access your information.

The first visit you make to the Barnes-Jewish Hospital Web site places a "cookie" on your computer. A cookie is a file used to personalize the Web site for you based on your initial and subsequent visits. The cookie will allow you to see or not to see items upon subsequent visits. This technology is not intended to identify you to us in any way; however, it can be used to serve ads to you based on your visit to our site. Click here to learn more about opting out of data collection by Google Analytics, or, click here to customize Google display network ad settings for your browser.

Disclaimer

The Barnes-Jewish Hospital Web site is intended as a reference and information source only. If you suspect you have a health problem, you should seek immediate care with the appropriate health care professionals. The information in this Web site is not a substitute for professional care and must not be used for self-diagnosis or treatment. Any links or pointers in this Web site are provided only as a courtesy. Barnes-Jewish Hospital assumes no liability for the information

EXHIBIT J-2

HIPAA NOTICE FOR THE MEDICAL CENTER

BARNES-JEWISH HOSPITAL, WASHINGTON UNIVERSITY SCHOOL OF MEDICINE, ST. LOUIS CHILDREN'S HOSPITAL

BJC HealthCare | 4444 Forest Park Avenue | St. Louis, Missouri 63108 USA | phone -- 314.747.WEBB

JOINT NOTICE OF PRIVACY PRACTICES

Effective Date: April 2003
Last Revision Date: July 2015
Effective Date Following Revision: November 5, 2015

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice serves as a joint notice for Barnes-Jewish Hospital, St. Louis Children's Hospital and Washington University School of Medicine (collectively referred to herein as "we" or "our" or "us"). Because we are affiliated health care providers, we have designated ourselves as an organized health care arrangement under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. We will follow the terms of this Notice and may share health information with each other for purposes of treatment, payment and health care operations as described in this Notice. Since we maintain health information separately, we will respond separately to your questions, requests and complaints concerning your health information.

OUR DUTIES REGARDING YOUR HEALTH INFORMATION

We are required by law to protect the privacy of your protected health information, to provide you with notice of these legal duties and to notify you following a breach of unsecured protected health information. This Notice explains how, when and why we typically use and disclose health information and your privacy rights regarding your health information. In our Notice, we refer to our uses and disclosures of health information as

our “Privacy Practices.” Protected health information generally includes information that we create or receive that identifies you and your past, present or future health status or care, or the provision of or payment for that health care. We are obligated to abide by these Privacy Practices as of the effective dates listed below.

WHO WILL FOLLOW THIS NOTICE

Our Notice serves as a Joint Notice and we will follow the terms of this Notice. This Notice, however, also describes the Privacy Practices of BJC HealthCare and its wholly owned subsidiaries and affiliated facilities described in the attached list and personnel (“BJC affiliated sites”), the Privacy Practices of Washington University School of Medicine and its wholly owned subsidiaries and affiliated facilities described in the attached list and their respective personnel, including Washington University Clinical Associates, L.L.C. and its wholly owned subsidiaries, affiliated practices and their respective personnel (“WUCA”).

Specifically, our Notice also describes the Privacy Practices of:

- Any BJC HealthCare affiliated hospital or service, all departments and units of our affiliated hospitals, and the health care professionals and other BJC HealthCare affiliated hospital personnel, including those employees or personnel of any other BJC HealthCare affiliated sites
- All Washington University School of Medicine health care providers, their staff and affiliated practices
- Any member of a volunteer group we allow to help you while you are receiving care from us

CHANGES TO THIS NOTICE

We reserve the right to change our Privacy Practices and the terms of this Notice. We will provide you with any revised Notice by making it available to you upon request and by posting it at our service sites. We will also post the revised Notice on our websites. Any changes that we make in our Privacy Practices will affect any protected health information that we maintain.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU WITHOUT YOUR WRITTEN CONSENT OR AUTHORIZATION

For Treatment, Payment and Health Care Operations

1. **For Your Treatment.** We may use and/or disclose your health information to health care providers and other personnel who are involved in your care and who will provide you with medical treatment or services. For example, if you have had surgery or just had a baby, we may contact a home health care agency to arrange for home services or to check on your recovery after you are discharged from the hospital.

2. **For Payment of Health Services.** We may use and/or disclose your health information to bill and receive payment for the services that you receive from us. For example, we may provide your health information to our billing or claims department to prepare a bill or statement to send to you, your insurance company, including Medicare or Medicaid, or another group or individual that may be responsible to pay for your health services.

3. **For Our Health Care Operations.** We may use or disclose your health information to carry out certain administrative, financial, legal and quality improvement activities that are necessary to run our businesses and to support our treatment and payment activities. For example, we may use and/or disclose your health information to help assess the quality and performance of our physicians and staff and improve the services that we provide. Specifically, we may disclose your health information to physicians, medical or other health or business professionals for review, consultation, comparison and planning. We may use and disclose your health information in the course of our training programs and for accreditation, certification, licensing or credentialing activities. Additionally, we may disclose your health information to auditors, accountants, attorneys, government regulators or other consultants to assess and/or ensure our compliance with laws or to represent us before regulatory or other governing authorities or judicial bodies.

4. **Special Circumstances When We May Disclose Your Health Information on a Limited Basis.** After removing direct identifying information (such as your name, address and Social Security number), we may use your health information for research, public health activities and other health care operations (such as business planning). While only limited identifying information will be used, we will also obtain assurances from the recipient of such health information that they will safeguard the information and only use and disclose the information for limited purposes.

   In conducting or participating in activities related to treatment, payment and health care operations, we may add or combine your information into electronic (computer) databases with information from other health care providers to help us improve our health services. For instance, using a combined information database, we may have more information to help us make more informed decisions about the range of treatments and care that may be available to you, including avoiding duplicate tests or conflicting treatment decisions. While we may not notify you about the inclusion of your data into these databases, you may be permitted to "opt-out" of some of these databases. We will make reasonable attempts to notify our patients, and perhaps the general public, of such opt-out options (when available) by posting notices in our facilities, on our websites or through social media.

For Activities Permitted or Required by Law

There are situations where we may use and/or disclose your health information without first obtaining your written authorization for purposes other than for treatment, payment or health care operations. Except for the specific situations where the law requires us to use and disclose information (such as reports of births to the health department or reports of abuse or neglect to social services), we have listed all these permitted uses and disclosures in this section.

1. **Public Health Activities.** We may disclose your health information to a public health authority that is authorized by law to collect or receive information in order to report, among other things, communicable diseases and child abuse, or to the U.S. Food and Drug Administration (FDA) to report medical device or product-related events. In certain limited situations, we may also disclose your health information to notify a person exposed to a communicable disease.

2. **Health Oversight Activities.** We may disclose your health information to a health oversight agency that includes, among others, an agency of the federal or state government that is authorized by law to monitor the health care system.

3. **Law Enforcement Activities.** We may disclose your health information in response to a law enforcement official's request for information to identify or locate a victim, a suspect, a fugitive, a material witness or a missing person (including individuals who have died) or for reporting a crime that has occurred on our premises or that may have caused a need for emergency services.

4. **Judicial and Administrative Proceedings.** We may disclose your health information in response to a subpoena or order of a court or administrative tribunal.

5. **Coroners, Medical Examiners and Funeral Directors.** We may disclose your health information to coroners, medical examiners and funeral directors to identify a deceased person or to determine the cause of death.

6. **Organ Donation.** We may disclose your health information to an organ procurement organization or other facility that participates in or makes a determination for the procurement, banking and/or transplantation of organs or tissues.

7. **Research Purposes.** We conduct and participate in medical, social, psychological and other types of research. Most human subject research projects, including many of those involving the use of health information, are subject to a special approval process which evaluates the proposed research project and its use of health information. In certain circumstances, however, we may disclose health information to researchers preparing to conduct a research project to help them determine whether a research project can be carried out or will be useful, so long as the health information they review does not leave our premises.

   Our clinicians may offer you the opportunity to participate in a clinical research trial (investigational treatments) and other researchers may contact you regarding your interest in participating in research projects. Your enrollment in a research project will occur only after you have been informed about the research, had an opportunity to ask questions and have signed a consent form. When approved through a special review process, research may be performed using your health information without your consent.

8. **Avoidance of Harm to a Person or Public Safety.** We may disclose if we believe that the disclosure is necessary to prevent or lessen a serious threat or harm to the public or the health or safety of another person.

9. **Specialized Government Functions.** We may disclose for specific governmental security needs, or as needed by correctional institutions.

10. **Workers' Compensation Purposes.** We may disclose to comply with workers' compensation laws or similar programs.

11. **Appointment Reminders and to Inform You of Health Related Products or Services.** We may use or disclose your health information to contact you for medical appointments or other scheduled services, or to provide you with information about treatment alternatives or other health-related benefits and services.

12. **Billing and Collection Purposes.** We may use or disclose your health information for the purpose of obtaining payment for services provided. You may be contacted by mail or telephone at any telephone number associated with you, including wireless numbers. Telephone calls may be made using pre-recorded or artificial voice messages and/or automatic dialing device (an "autodialer"). Messages may be left on answering machines or voicemail, including any such message information required by law (including debt collection laws) and/or regarding amounts owed by you. Text messages or emails using any email addresses you provide may also be used in order to contact you.

13. **Fundraising Purposes.** We may use or disclose demographic information, including names, addresses, other contact information, age, gender and date of birth; the dates that you received health care from us; department of service information; treating physician information; and outcome information to contact you in order to raise funds so that we may continue or expand our health care activities. You have the right to opt out of these fundraising activities. If you do not wish to be contacted as part of our fundraising efforts, please contact the individual(s) listed in the Contact Section of this Notice. If you decide you do not wish to be contacted as part of our fundraising efforts, we will not condition service or payment upon that decision.

When your preferences will guide our use or disclosure

1. A facility directory may include your name, your location in the facility, your general condition such as fair, stable, etc., and your religious affiliation (if provided by you). Unless you tell us that you would like to restrict your information in a facility directory, you will be included and directory information may be disclosed to members of the clergy or to people who ask for you by name.
2. We may disclose your health information to a family member, other relative, friend or any other person you identify who is involved in your care or involved with the payment related to your care unless you tell us otherwise.

Uses and Disclosures that Require Your Prior Written Authorization

1. We will not disclose psychotherapy notes without your written authorization unless the use and disclosure is otherwise permitted or required by law.

2. We will not engage in disclosures that constitute a sale of your health information without your written authorization. A sale of protected health information occurs when we, or someone we contract with directly or indirectly, receive payment in exchange for your protected health information.

3. We will not use or disclose your protected health information for marketing purposes without your written authorization. Marketing is defined as receipt of payment from a third party for communicating with you about a product or service marketed by the third party.

For situations not generally described in our Notice, we will ask for your written authorization before we use or disclose your health information. You may revoke that authorization, in writing, at any time to stop future disclosures of your health information. Information previously disclosed, however, will not be requested to be returned nor will your revocation affect any action that we have already taken in reliance on your

authorization. In addition, if we collected the information in connection with a research study, we are permitted to use and disclose that information to the extent it is necessary to protect the integrity of the research study.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

Requesting Restrictions of Certain Uses and Disclosures of Health Information
You may request, in writing, a restriction on how we use or disclose your protected health information for your treatment, for payment of your health care services, or for activities related to our health care operations. You may also request a restriction on what health information we may disclose to someone who is involved in your care, such as a family member or friend. To make a request, see contact information below.

We are not required to agree to your request in all circumstances. Additionally, any restriction that we may approve will not affect any use or disclosure that we are required or permitted to make under the law. We must agree to your request to restrict disclosure of your health information to your health plan if the disclosure is not required by law and the health information you want restricted pertains solely to a health care item or service for which you (or someone other than your health plan, on your behalf) have paid us for in full.

Requesting Confidential Communications
You may request changes in the manner in which we communicate with you or the location where we may contact you. You must make your request in writing. See contact information below. We will accommodate your reasonable request, but in determining whether your request is reasonable, we may consider the administrative difficulty it may impose on us.

Inspecting and Obtaining Copies of Your Health Information
You may ask to look at and obtain a copy of your health information. You must make your request in writing. See contact information at the end of this notice.

We may charge a fee for copying or preparing a summary of requested health information. We will respond to your request for health information within 30 days of receiving your request by either providing the information requested, denying the request with a written explanation for the denial, or advising you we need additional time to complete our action on your request (for instance, if your health information is not readily accessible or the information is maintained in an off-site storage location).

Requesting a Change in Your Health Information
You may request, in writing, a change or addition to your health information. See contact information below. The law limits your ability to change or add to your health information. These limitations include whether we created or include the health information within our medical records or if we believe that the health information is accurate and complete without any changes. Under no circumstances will we erase or otherwise delete original documentation in your health information.

Requesting an Accounting of Disclosures of Your Health Information
You may ask, in writing, for an accounting of certain types of disclosures of your health information. The law excludes from an accounting many of the typical disclosures, such as those made to care for you, to pay for your health services, or where you provided your written authorization to the disclosure.

To make a request for an accounting see contact information below. Generally, we will respond to your request within 60 days of receiving your request unless we need additional time.

Notification Following a Breach of Unsecured Protected Health Information
We will notify you within a reasonable time not to exceed 60 days, in writing, in the event your health information is compromised by BJC HealthCare, Washington University School of Medicine, one of our affiliates or by someone with whom we contracted to conduct business on our behalf.

Obtaining a Notice of Our Privacy Practices
We provide you with our Notice to explain and inform you of our Privacy Practices. You may also take a copy of this Notice with you. Even if you have requested this Notice electronically, you may request a paper copy at any time. You may also view or obtain a copy of this Notice at our websites: BJC HealthCare (http://www.bjc.org/Default.aspx) and Washington University School of Medicine (http://www.wuphysicians.wustl.edu/).

COMPLAINTS
We welcome an opportunity to address any concerns that you may have regarding the privacy of your health information. If you believe that the privacy of your health information has been violated, you may file a complaint with the individuals listed in the Contact Section of this Notice. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services.

You will not be penalized or retaliated against for filing a complaint.

CONTACT INFORMATION
It is important to note that requests to Barnes-Jewish Hospital, St. Louis Children's Hospital and Washington University must be made separately. Any requests or complaints to one provider will not be deemed to be filed with any of the other providers covered by or addressed in this Joint Notice.

For questions, concerns, requests or complaints concerning Barnes-Jewish Hospital or St. Louis Children's Hospital, please contact the Barnes- Jewish Hospital operator at (314) 362-5000 or St. Louis Children's Hospital operator at (314) 454-6000 and request the Patient Liaison/Advocate or write to the Patient Liaison/Advocate at the address shown below.

For questions, concerns, requests or complaints concerning Washington University or its providers, you may contact the Privacy Officer at the telephone number or address listed below. To look at or obtain a copy or your health information from a Washington University physician or provider, you may contact the Washington University Health Information Release Service at (314) 273-0453.

Barnes-Jewish Hospital
Patient Liaison

Address: Office of Patient & Family Affairs
Attention: Patient Liaison
Mail Stop: 90-72-432
One Barnes-Jewish Hospital Plaza
St. Louis, Missouri 63110 USA

Telephone Number: (314) 362-6100

St. Louis Children's Hospital
Patient Liaison

Address: Attn: Patient Advocacy Coordinator
One Children's Place, Suite 4S50
St. Louis, Missouri 63110 USA

Telephone Number: (314) 286-0711

Washington University
Privacy Officer

Address: Campus Box 8098
660 South Euclid Avenue
St. Louis, Missouri 63110 USA

Telephone Number: toll-free (866) 747-4975

BJC HEALTHCARE SERVICE DELIVERY SITES

BJC HealthCare Hospitals

Alton Memorial Hospital
Barnes-Jewish Hospital
Barnes-Jewish St. Peters Hospital
Barnes-Jewish West County Hospital
Boone Hospital Center
Christian Hospital and Northwest HealthCare
Missouri Baptist Medical Center
Missouri Baptist Sullivan
Parkland Health Center - Bonne Terre
Parkland Health Center - Farmington
Parkland Health Center - Weber Road
Progress West Hospital
St. Louis Children's Hospital

BJC HealthCare Long-Term Care Facilities

Barnes-Jewish Extended Care
Eunice Smith Nursing Home

BJC HEALTH SERVICES

BJC Behavioral Health
BJC Corporate Health Services
BJC Home Care Services and Boone Hospital Home Care and Hospice
BJC Medical Group Offices
BJC Retail Pharmacies
BJC Vision Centers

Fairview Heights Medical Group
Heart Care Institute
Siteman Cancer Center

For more information concerning BJC HealthCare facility locations, please visit our website at www.bjc.org (http://www.bjc.org) or call (314) 362-9355 or 1-800-392-0936.

WASHINGTON UNIVERSITY CLINICAL ASSOCIATES SERVICE DELIVERY SITES

Blue Fish Pediatrics
Cloverleaf Pediatrics
Forest Park Pediatrics
Grant Medical Group
Maryland Medical Group
Northwest Pediatrics
O'Fallon Pediatrics
University Internal Medicine and Diabetes Associates
WUCA Child Neurology Associates

LARGE PRINT

Large Print HIPAA pdf (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin-LARGE-PRINT.pdf)

AUDIO FILE

Audio File (https://clyp.it/1sgzcztk)

TRANSLATIONS

American Sign Language (https://youtu.be/m54Uf9KCL30)

Please click on the links below to view .pdf files of this content in multiple languages:

- Arabic (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_ARABIC.pdf)
- Bosnian (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_BOSNIAN.pdf)
- Farsi (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_FARSI.pdf)
- German (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_GERMAN.pdf)
- Nepali (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_NEPALI.pdf)
- Russian (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_RUSSIAN.pdf)
- Spanish (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_SPANISH.pdf)
- Chinese (Simplified) (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_SIMPLIFIED CHINESE.pdf)
- Vietnamese (/Portals/0/Legal/BJC22095_NPP-CENTRAL_fin_VIETNAMESE.pdf)

Legal (http://www.barnesjewish.org/Legal)

HIPAA Notice for the Medical Center (http://www.barnesjewish.org/Legal/HIPAA-Notice-for-the-Medical-Center)

Important Information for Vendors (http://www.bjc.org/About-Us/Vendor-Information)

Joint Commission Public Notice Regarding Safety & Quality of Care (http://www.barnesjewish.org/Legal/Joint-Commission-Public-Notice-Regarding-Safety-Quality-of-Care)

(http: (http: (http: (http:

SIGN UP TODAY FOR FREE E-NEWSLETTERS

Enter Your Email Address SIGN UP

MORE OPTIONS > (/ABOUT-US/E-NEWSLETTER)

FIND A DOCTOR OR MAKE AN APPOINTMENT: (TEL:)(855) 925-0631

GENERAL INFORMATION: 314.747.3000 (TEL:3147473000)

PATIENT CARE +

ABOUT US +

CAREERS +

FOR PROFESSIONALS +

WHAT'S NEW +

(http://wuphysicians.wustl.edu/)

One Barnes-Jewish Hospital Plaza
St. Louis, MO 63110

Home (/) Legal (/Legal) HIPAA (/Legal/HIPAA-Notice-for-the-Medical-Center) Sitemap (/Sitemaps)

BACK TO TOP ^

LEGAL

TERMS OF USE AND PRIVACY STATEMENT

TERMS OF USE

Barnes-Jewish Hospital or the "Site Sponsor"), is providing information and services on this Internet site as a benefit to our users. The information and services on this site are provided solely for general illustration, educational and resource provision purposes. Such information and services are not intended to be specific medical, health, business or other professional advice or direction. If you have specific questions regarding your health or health status, contact your physician or other health care provider. Neither the Site Sponsor nor its information contributors make any express or implied representations or warranties about the completeness or accuracy of this information and these services for any purpose or the suitability of this information or these services for any particular use.

This site will also enable users to obtain information on the services, events and materials offered, happening or available through the Site Sponsor, including publications and educational programs, current news, certain Barnes-Jewish Hospital, BJC HealthCare and Washington University School of Medicine documents, press releases, lists of health related web sites, and other information relevant to purposes of this site.

This internet site may include "links" providing direct access to other Internet sites. However, the Site Sponsor takes no responsibility for the content or information contained on those other sites, and does not exert any editorial, monitoring or other control over those other sites and therefore do not assume any liability for those sites or their content. The Site Sponsor reserves the right to remove any link from this site for any or no reason. The existence of any particular link is simply intended to imply potential interest to users of this site.

Certain areas of the site may allow for the posting or exchange of information among and between users. Users that submit or post information to this site grant the Site Sponsor the authority and right to use any submission in any way, and by such submissions warrant and represent to the Site Sponsor that such submissions are not in violation of United States copyright or other laws. In addition, the Site Sponsor reserves the right to review, edit or delete any posting or information (including, without limitation, those that appear to be inappropriate for the intended purposes of this site). Note: Any information that you include in your posting will be posted to the bulletin board and be available to any or all users, including without limitation, personal, health and demographic information.

All images, text, and other materials posted on this site are subject to copyrights owned by the Site Sponsor or other individuals or entities and are protected by United States copyright laws. Any reproduction, retransmission, distribution or republication of all or part of any images, text programs, and other materials

found on this site is expressly prohibited, unless the Site Sponsor or the copyright owner of the material has expressly granted its prior written consent. All other rights reserved. This site is intended to be maintained in a manner consistent with United States copyright laws. Accordingly, users should not submit or post copyrighted material to this site unless the copyright owner of the material has expressly granted its prior written consent to such submission.

All trademarks, service marks and logos referred to or appearing on this site are the property of their respective owners. The names, trademarks, service marks and logos of the Site Sponsor appearing on this site may not be used in any advertising or publicity, or otherwise to indicate sponsorship of or affiliation with any product or service, without the applicable Site Sponsor's prior express written permission.

PRIVACY STATEMENT

Barnes-Jewish Hospital has created this statement to demonstrate our commitment to your privacy. This statement explains our information-gathering and dissemination practices for this Web site.

A typical visit to our Web site does not require a user to submit personal information. However, if you decide to send us an e-mail, respond to a survey, or subscribe to an online publication with your contact information, we will respond to you with the information you request and other information that we think might be of interest to you. If you choose to receive more information, your name and contact information (including e-mail address) will be added to our database. From that database, we may send you materials such as newsletters, brochures or articles of interest via regular mail, e-mail or in other ways.

Information you submit may be routinely shared with our parent organization, BJC HealthCare as they often distribute our materials, or with the Washington University School of Medicine if you are looking for a physician referral. Other than these two organizations, we will only forward your personal information to organizations working on our behalf. We urge you not to provide any confidential information about you or your health to us via electronic communication. If you do so, it is at your own risk. Although we attempt to maintain our computer network in a secure manner to protect the content of your messages, we cannot provide absolute assurance that the contents of your e-mail will not become accessible to individuals or entities that are not authorized to access your information.

The first visit you make to the Barnes-Jewish Hospital Web site places a "cookie" on your computer. A cookie is a file used to personalize the Web site for you based on your initial and subsequent visits. The cookie will allow you to see or not to see items upon subsequent visits. This technology is not intended to identify you to us in any way; however, it can be used to serve ads to you based on your visit to our site. Click here (https://tools.google.com/dlpage/gaoptout/) to learn more about opting out of data collection by Google Analytics, or, click here (https://www.google.com/settings/ads) to customize Google display network ad settings for your browser.

DISCLAIMER

The Barnes-Jewish Hospital Web site is intended as a reference and information source only. If you suspect you have a health problem, you should seek immediate care with the appropriate health care professionals. The information in this Web site is not a substitute for professional care and must not be used for self-diagnosis or treatment. Any links or pointers in this Web site are provided only as a courtesy. Barnes-Jewish Hospital assumes no liability for the information contained in this Web site or for its use.

Legal (http://www.barnesjewish.org/Legal)

HIPAA Notice for the Medical Center (http://www.barnesjewish.org/Legal/HIPAA-Notice-for-the-Medical-Center)

Important Information for Vendors (http://www.bjc.org/About-Us/Vendor-Information)

Joint Commission Public Notice Regarding Safety & Quality of Care (http://www.barnesjewish.org/Legal/Joint-Commission-Public-Notice-Regarding-Safety-Quality-of-Care)

(http: (http: (http: (http:

FIND A DOCTOR OR MAKE AN APPOINTMENT: (TEL:)(855) 925-0631

GENERAL INFORMATION: 314.747.3000 (TEL:3147473000)

PATIENT CARE +

ABOUT US +

CAREERS +

FOR PROFESSIONALS +

WHAT'S NEW +

(http://wuphysicians.wustl.edu/)

One Barnes-Jewish Hospital Plaza
St. Louis, MO 63110

Home (/) Legal (/Legal) HIPAA (/Legal/HIPAA-Notice-for-the-Medical-Center) Sitemap (/Sitemaps)

BACK TO TOP

EXHIBIT K-1

<LINK: http://my.clevelandclinic.org/ >

Cleveland Clinic

Privacy & Security

Privacy Policy | **Security Statement**

Cleveland Clinic's mission is, and always will be, "Patients First". We understand, acknowledge and respect any individual's right to privacy and the concerns one may have in regard to privacy and security. We recognize the importance of protecting the privacy of information provided by our patients, as well as, general users of our website.

IMPORTANT NOTE! The Cleveland Clinic Notice of Privacy Practices is a separate document that governs how medical information about you may be used and disclosed by Cleveland Clinic.

MEDICAL DISCLAIMER. IF THIS IS A MEDICAL EMERGENCY, PLEASE IMMEDIATELY CALL EMERGENCY PERSONNEL (911) TO GET PROMPT MEDICAL ATTENTION. DO NOT RELY ON ELECTRONIC COMMUNICATIONS FOR ASSISTANCE IN REGARD TO YOUR IMMEDIATE, URGENT MEDICAL NEEDS. THIS E-MAIL IS NOT DESIGNED TO FACILITATE MEDICAL EMERGENCIES. CLEVELAND CLINIC CANNOT GUARANTEE RESPONSE TIMES IF YOU CHOOSE TO USE THIS E-MAIL IN THE EVENT OF A MEDICAL EMERGENCY.

PERSONAL INFORMATION.

A visitor can access and browse our entire site at any time without providing any personal information. We do not collect information that would personally identify you unless you choose to provide it.

In addition, Cleveland Clinic does not share any personally identifiable information of any individual with any third party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization.

Forms

Our website contains forms through which users may request information or supply feedback to us. In some cases, telephone numbers, email addresses or return addresses are required so that we can supply requested information to you, and in other cases, correct names and addresses are required to process credit card payments.

After you fill out a form, we may contact you with follow-up information (unless you have checked an "opt-out" box on the form). We do not provide any information supplied on our web forms to any outside organization for any reason (other than where we may be required to by law, or as necessary to process credit card information). We do not save this personal information for any other reason.

Surveys

Occasionally, we may survey visitors to our site. The information from these surveys is used in aggregate form to help us understand the needs of our visitors so that we can improve our site. We generally do not ask for information in surveys that would personally identify you. If we do request contact information for follow-up, you may decline to provide it. If survey respondents provide personal information (such as an email address) in a survey, it is shared only with those people who need to see it to respond to the question or request.

Email

"Phishing" is a scam designed to steal your personal information. If you receive an email that looks like it is from Cleveland Clinic asking you for your personal information, do not respond. We will never request your password, user name, credit card information or other personal information through email.

User Name and Password

In the event you access any Service requiring a User Name and Password, you are solely responsible for keeping such User Name and Password strictly confidential.

NON-PERSONAL INFORMATION

Cleveland Clinic collects non-personal information such as website usage, traffic patterns, site performance and related statistics based on our tracking of your visits to the website.

IP Addresses

The Web server automatically collects the IP (which stands for Internet Protocol) address of the computers that access our site. An IP address is a number that is assigned to your computer when you access the Internet. It is not truly personally identifiable information because many different individuals can access the Internet via the same computer. We use this information in aggregate form to understand how our site is being used and how we can better serve visitors.

Please note that although such information is not personally identifiable, we can determine from an IP address a visitor's Internet Service Provider and the geographic location of his or her point of connectivity.

First Party Cookies

We collect information about visitors to our site using "first party cookies", which are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser. Cookies are never associated with specific personal identities. First party cookies are distinct from third party cookies that they are created and directly served by the company hosting the website.

We use two types of "cookies" on this site:

- We use persistent cookies to recognize a repeat visitor, enabling us the opportunity to offer the visitor a set of services or information requested in a previous visit.
- We use session cookies to track a visitor's path through our site during a visit, to help us understand how people use our site.

You can delete our cookies at any time. The "help" section, located on the toolbar of most browsers, will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie or how to disable cookies altogether. Since cookies allow you to take full advantage of some of our website's best features, we recommend that you leave them turned on.

SECURITY OF YOUR INFORMATION

Please note that our forms are encrypted to protect your privacy. Once the information is sent to our site, it is kept in secure databases where it is not available to users on the Internet. While we sometimes ask for credit card numbers or certain service transactions, and either pass them on to a credit card processing service or process them manually, we do not store credit card numbers online.

Cleveland Clinic periodically reviews and modifies, where appropriate, its security policies and procedures. We use reasonable care to protect your personally identifiable and confidential information provided by you to our site. Cleveland Clinic has in place a security program that seeks to mitigate this risk substantially.

DISCLAIMER OF WARRANTY

MATERIALS, SERVICES AND OTHER INFORMATION ARE PROVIDED "AS IS" BY CLEVELAND CLINIC FOR EDUCATIONAL PURPOSES ONLY. CLEVELAND CLINIC MAKES NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, TITLE OR NON INFRINGEMENT.

PLEASE NOTE THAT, BY ITS VERY NATURE, A WEBSITE CANNOT BE ABSOLUTELY PROTECTED AGAINST INTENTIONAL OR MALICIOUS INTRUSION ATTEMPTS. FURTHERMORE, CLEVELAND CLINIC DOES NOT CONTROL THE DEVICES OR COMPUTERS OR THE INTERNET OVER WHICH YOU MAY CHOOSE TO SEND CONFIDENTIAL PERSONAL INFORMATION AND CANNOT, THEREFORE, PREVENT SUCH INTERCEPTIONS OF COMPROMISES TO YOUR INFORMATION WHILE IN TRANSIT TO CLEVELAND CLINIC.

THEREFORE, CLEVELAND CLINIC HEREBY MAKES NO GUARANTEE AS TO SECURITY, INTEGRITY OR CONFIDENTIALITY OF ANY INFORMATION TRANSMITTED TO OR FROM THIS WEBSITE, OR STORED WITHIN THIS WEBSITE.

BEYOND OUR REASONABLE CARE TO SAFEGUARD YOUR INFORMATION WHILE IN TRANSIT, CLEVELAND CLINIC CANNOT AND DOES NOT GUARANTEE THE ABSOLUTE SECURITY OF ELECTRONIC COMMUNICATIONS OR TRANSMISSIONS SINCE ANY TRANSMISSION MADE OVER THE INTERNET BY ANY ORGANIZATION OR ANY INDIVIDUAL RUNS THE RISK OF INTERCEPTION.

IN ADDITION, WE HEREBY MAKE NO GUARANTEE AS TO SECURITY, INTEGRITY OR CONFIDENTIALITY OF ANY INFORMATION TRANSMITTED TO OR FROM THIS WEBSITE, OR STORED WITHIN THIS WEBSITE.

LIMITATION OF LIABILITY

YOU ASSUME THE SOLE RISK OF TRANSMITTING YOUR INFORMATION AS IT RELATES TO THE USE OF THIS WEBSITE, AND FOR ANY DATA CORRUPTIONS, INTENTIONAL INTERCEPTIONS, INTRUSIONS OR UNAUTHORIZED ACCESS TO INFORMATION, OR OF ANY DELAYS, INTERRUPTIONS TO OR FAILURES PREVENTING THE USE THIS WEBSITE.

IN NO EVENT SHALL CLEVELAND CLINIC BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL OR MONETARY DAMAGES, INCLUDING FEES, AND PENALTIES IN CONNECTION WITH YOUR USE OF MATERIALS POSTED ON THIS SITE OR CONNECTIVITY TO OR FROM THIS SITE TO ANY OTHER SITE.

CLEVELAND CLINIC MAY CHANGE THIS PRIVACY POLICY WITHOUT NOTICE TO YOU.

Other services provided by Cleveland Clinic on this Website may require you to agree to additional terms.

BY USING THIS WEBSITE, YOU ACCEPT THESE TERMS.

If you have any questions about our privacy policy or our use of information gathered through our Web site, please contact our Webmaster at webmail@ccf.org.

Last updated: 3/18/2009

Cleveland Clinic values your privacy and security. Your data is protected through Secure Socket Layer (SSL) 128-bit encryption, ensuring your confidential information is protected using both server authentication and data encryption technology.

- For more information, please review our Website Terms of Use <LINK: http://my.clevelandclinic.org/about-cleveland-clinic/about-this-website/terms-of-use.aspx > and Website Privacy Policy.

EXHIBIT K-2

<LINK: http://my.clevelandclinic.org/ >

Cleveland Clinic

Privacy & Security

Privacy Policy | **Security Statement**

Cleveland Clinic's mission is, and always will be, "Patients First". We understand, acknowledge and respect any individual's right to privacy and the concerns one may have in regard to privacy and security. We recognize the importance of protecting the privacy of information provided by our patients, as well as, general users of our website.

IMPORTANT NOTE! The Cleveland Clinic Notice of Privacy Practices is a separate document that governs how medical information about you may be used and disclosed by Cleveland Clinic.

MEDICAL DISCLAIMER. IF THIS IS A MEDICAL EMERGENCY, PLEASE IMMEDIATELY CALL EMERGENCY PERSONNEL (911) TO GET PROMPT MEDICAL ATTENTION. DO NOT RELY ON ELECTRONIC COMMUNICATIONS FOR ASSISTANCE IN REGARD TO YOUR IMMEDIATE, URGENT MEDICAL NEEDS. THIS E-MAIL IS NOT DESIGNED TO FACILITATE MEDICAL EMERGENCIES. CLEVELAND CLINIC CANNOT GUARANTEE RESPONSE TIMES IF YOU CHOOSE TO USE THIS E-MAIL IN THE EVENT OF A MEDICAL EMERGENCY.

PERSONAL INFORMATION.

A visitor can access and browse our entire site at any time without providing any personal information. We do not collect information that would personally identify you unless you choose to provide it.

In addition, Cleveland Clinic does not share any personally identifiable information of any individual with any third party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization.

Forms

Our website contains forms through which users may request information or supply feedback to us. In some cases, telephone numbers, email addresses or return addresses are required so that we can supply requested information to you, and in other cases, correct names and addresses are required to process credit card payments.

After you fill out a form, we may contact you with follow-up information (unless you have checked an "opt-out" box on the form). We do not provide any information supplied on our web forms to any outside organization for any reason (other than where we may be required to by law, or as necessary to process credit card information). We do not save this personal information for any other reason.

Surveys

Occasionally, we may survey visitors to our site. The information from these surveys is used in aggregate form to help us understand the needs of our visitors so that we can improve our site. We generally do not ask for information in surveys that would personally identify you. If we do request contact information for follow-up, you may decline to provide it. If survey respondents provide personal information (such as an email address) in a survey, it is shared only with those people who need to see it to respond to the question or request.

Email

"Phishing" is a scam designed to steal your personal information. If you receive an email that looks like it is from Cleveland Clinic asking you for your personal information, do not respond. We will never request your password, user name, credit card information or other personal information through email.

User Name and Password

In the event you access any Service requiring a User Name and Password, you are solely responsible for keeping such User Name and Password strictly confidential.

NON-PERSONAL INFORMATION

Cleveland Clinic collects non-personal information such as website usage, traffic patterns, site performance and related statistics based on our tracking of your visits to the website.

IP Addresses

The Web server automatically collects the IP (which stands for Internet Protocol) address of the computers that access our site. An IP address is a number that is assigned to your computer when you access the Internet. It is not truly personally identifiable information because many different individuals can access the Internet via the same computer. We use this information in aggregate form to understand how our site is being used and how we can better serve visitors.

Please note that although such information is not personally identifiable, we can determine from an IP address a visitor's Internet Service Provider and the geographic location of his or her point of connectivity.

First Party Cookies

We collect information about visitors to our site using "first party cookies", which are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser. Cookies are never associated with specific personal identities. First party cookies are distinct from third party cookies that they are created and directly served by the company hosting the website.

We use two types of "cookies" on this site:

- We use persistent cookies to recognize a repeat visitor, enabling us the opportunity to offer the visitor a set of services or information requested in a previous visit.
- We use session cookies to track a visitor's path through our site during a visit, to help us understand how people use our site.

You can delete our cookies at any time. The "help" section, located on the toolbar of most browsers, will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie or how to disable cookies altogether. Since cookies allow you to take full advantage of some of our website's best features, we recommend that you leave them turned on.

SECURITY OF YOUR INFORMATION

Please note that our forms are encrypted to protect your privacy. Once the information is sent to our site, it is kept in secure databases where it is not available to users on the Internet. While we sometimes ask for credit card numbers or certain service transactions, and either pass them on to a credit card processing service or process them manually, we do not store credit card numbers online.

Cleveland Clinic periodically reviews and modifies, where appropriate, its security policies and procedures. We use reasonable care to protect your personally identifiable and confidential information provided by you to our site. Cleveland Clinic has in place a security program that seeks to mitigate this risk substantially.

DISCLAIMER OF WARRANTY

MATERIALS, SERVICES AND OTHER INFORMATION ARE PROVIDED "AS IS" BY CLEVELAND CLINIC FOR EDUCATIONAL PURPOSES ONLY. CLEVELAND CLINIC MAKES NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, TITLE OR NON INFRINGEMENT.

PLEASE NOTE THAT, BY ITS VERY NATURE, A WEBSITE CANNOT BE ABSOLUTELY PROTECTED AGAINST INTENTIONAL OR MALICIOUS INTRUSION ATTEMPTS. FURTHERMORE, CLEVELAND CLINIC DOES NOT CONTROL THE DEVICES OR COMPUTERS OR THE INTERNET OVER WHICH YOU MAY CHOOSE TO SEND CONFIDENTIAL PERSONAL INFORMATION AND CANNOT, THEREFORE, PREVENT SUCH INTERCEPTIONS OF COMPROMISES TO YOUR INFORMATION WHILE IN TRANSIT TO CLEVELAND CLINIC.

THEREFORE, CLEVELAND CLINIC HEREBY MAKES NO GUARANTEE AS TO SECURITY, INTEGRITY OR CONFIDENTIALITY OF ANY INFORMATION TRANSMITTED TO OR FROM THIS WEBSITE, OR STORED WITHIN THIS WEBSITE.

BEYOND OUR REASONABLE CARE TO SAFEGUARD YOUR INFORMATION WHILE IN TRANSIT, CLEVELAND CLINIC CANNOT AND DOES NOT GUARANTEE THE ABSOLUTE SECURITY OF ELECTRONIC COMMUNICATIONS OR TRANSMISSIONS SINCE ANY TRANSMISSION MADE OVER THE INTERNET BY ANY ORGANIZATION OR ANY INDIVIDUAL RUNS THE RISK OF INTERCEPTION.

IN ADDITION, WE HEREBY MAKE NO GUARANTEE AS TO SECURITY, INTEGRITY OR CONFIDENTIALITY OF ANY INFORMATION TRANSMITTED TO OR FROM THIS WEBSITE, OR STORED WITHIN THIS WEBSITE.

LIMITATION OF LIABILITY

YOU ASSUME THE SOLE RISK OF TRANSMITTING YOUR INFORMATION AS IT RELATES TO THE USE OF THIS WEBSITE, AND FOR ANY DATA CORRUPTIONS, INTENTIONAL INTERCEPTIONS, INTRUSIONS OR UNAUTHORIZED ACCESS TO INFORMATION, OR OF ANY DELAYS, INTERRUPTIONS TO OR FAILURES PREVENTING THE USE THIS WEBSITE.

IN NO EVENT SHALL CLEVELAND CLINIC BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL OR MONETARY DAMAGES, INCLUDING FEES, AND PENALTIES IN CONNECTION WITH YOUR USE OF MATERIALS POSTED ON THIS SITE OR CONNECTIVITY TO OR FROM THIS SITE TO ANY OTHER SITE.

CLEVELAND CLINIC MAY CHANGE THIS PRIVACY POLICY WITHOUT NOTICE TO YOU.

Other services provided by Cleveland Clinic on this Website may require you to agree to additional terms.

BY USING THIS WEBSITE, YOU ACCEPT THESE TERMS.

If you have any questions about our privacy policy or our use of information gathered through our Web site, please contact our Webmaster at webmail@ccf.org.

Last updated: 3/18/2009

Cleveland Clinic values your privacy and security. Your data is protected through Secure Socket Layer (SSL) 128-bit encryption, ensuring your confidential information is protected using both server authentication and data encryption technology.

- For more information, please review our Website Terms of Use <LINK: http://my.clevelandclinic.org/about-cleveland-clinic/about-this-website/terms-of-use.aspx > and Website Privacy Policy.

EXHIBIT L-1

THE UNIVERSITY OF TEXAS
MD Anderson
~~Cancer~~ Center

Making Cancer History®

About Us

Privacy Policy

This is how we handle the information we learn from you when you visit The University of Texas MD Anderson Cancer Center Web site (www.mdanderson.org). The information we receive depends on what you do during your visit.

Web Server

Our web server collects and stores the following general information about you:

- the name of the domain from which you access the Internet (for example, aol.com, if you are connecting from an America Online account);
- the date and time you access our service;
- the pages you visit;
- the Internet address of the Web site from which you linked directly to us.
- the name and release number of web browser software you are using.

This information is collected automatically and is not linked to your personal identity. It is used in an aggregate way to help us improve our Web site and make it more useful to you. This information may be shared with a third-party web analytics company.

Use of Cookies

Cookies are small files that many Web sites place on your hard drive that allow those Web sites to identify you. The use of cookies is a standard and common practice of many Web sites. For example, if you allow a Web site to remember your login name or password, the Web site places a cookie on your computer. We may place cookies on your computer to allow us to allow us to know when you are on our Web site during future visits. We may use cookies to measure web traffic, to offer you certain products or services, and to customize your visit. However, if you do not wish to receive cookies, or want to be notified of when they are placed, your internet browser may permit you to do so. In many internet browsers, you can change the browser settings to warn you before accepting cookies or to block cookies. If you block cookies, you may not be able to use certain Web site features or functions, or this Web site may not operate in an optimal mode.

Online Forms & Email Communication

We do not obtain personal information (e.g. name, address, e-mail address, etc.) about you when you visit the MD Anderson Web site unless you choose voluntarily to provide such information to us.

If you identify yourself by sending an e-mail, by using a form like "Contact Us," or by registering to receive information from us, there are a few things you should know.

- Various people at MD Anderson Cancer Center may see the material you submit.
- We may enter the information you send into our electronic database, to share with our physicians, other health care professionals, researchers, or our Internet services staff.
- In other limited circumstances, including requests from legal authorities, we may be required by law to disclose information you submit.

You should note that electronic mail and other Internet communications channels are not necessarily secure against interception. While we take precautions, such as encrypting communications where appropriate, if your communication is very sensitive, or includes information like your diagnosis or medical history, you might want to send it by postal mail instead.

Message Boards

Our patient message boards collect and store the following information about you:

- First Name, Last Name & Email Address
- Posted Messages
- The date and time you access the board

Patient communications on the message boards are not private and can be seen by a community of cancer discussion participants. Message boards offer a chance for patients to share concerns and ideas they have about cancer and its impact on their lives.

Under no circumstances will we ever disclose (to a third party) personal information about individual medical conditions or interests, except when we believe in good faith that the law requires it.

With few exceptions, you are entitled on your request to be informed about the information MD Anderson Cancer Center collects about you. Under Sections 552.021 and 552.023 of the Texas Government Code, you are entitled to receive and review the information. Under Section 559.004 of the Texas Government Code, you are entitled to have MD Anderson Cancer Center correct information about you that is held by us and that is incorrect, in accordance with the procedures set forth in The University of Texas System Business Procedures Memorandum 32. The information that MD Anderson Cancer Center collects will be retained and maintained as required by Texas records retention laws (Section 441.180 et seq. of the Texas Government Code) and rules. Different types of information are kept for different periods of time.

From time to time, this Web site may provide links to other useful or interesting Web sites that are not owned or controlled by MD Anderson Cancer Center. We cannot be responsible for the content or privacy practices used by other Web site owners.

You may contact us with any questions or comments about our privacy policy.

EXHIBIT L-2

THE UNIVERSITY OF TEXAS MD Anderson Cancer Center

MENU

Privacy Policy

Effective Date: September 8, 2016

This Privacy Policy describes how The University of Texas MD Anderson Cancer Center ("MD Anderson," "we," "us," or "our") collects, uses, and shares information about you that we obtain through mdanderson.org and makingcancerhistory.com (the "Sites"). This Privacy Policy does not apply to our offline data collection activities, unless otherwise stated below or at the time of collection.

The practices described in this Privacy Policy are not applied to protected health information. Our privacy practices regarding protected health information are described in our Joint Notice of Privacy Practices. With respect to information you submit through the "request an appointment" form on the Sites, once we have accepted such information, our handling of that information is governed by the Joint Notice of Privacy Practices.

Information collection

Information You Provide To Us

We collect information you provide directly to us through the Sites. For example, we collect information when you create an account, subscribe to receive notifications, make a donation, apply for a job, or otherwise communicate with us through the Sites.

The information we collect from you may include personal information. "Personal Information" is information that, whether alone or in combination with other information, can be used to identify an individual (such as first and last name, e-mail address, home address, telephone number, or date of birth). Information that has been de-identified such that it cannot be connected to an individual is not considered Personal Information for purposes of this Privacy Policy.

Information We Collect Automatically

When you access or use the Sites, certain information about your use of the Sites may be collected automatically. For example, we may collect your IP address, device identifier, browser type, domain name, operating system characteristics, data regarding the device you're using, and information about your visit, such as access times, duration, and how you arrived at the Sites. This usage information may be combined with Personal Information, in which case we would treat the combined information as Personal Information.

In addition to logging information about your visit, we may use various tracking mechanisms such as cookies, web beacons (also known as tracking pixels), and embedded scripts (collectively, "Tracking Technologies") to automatically collect information about interactions with our Sites or e-mails.

- **Cookies** are small text files that a web page server places on your hard drive. The use of cookies is a common practice on many websites. We may place cookies on your computer to allow us to recognize you on the Sites during future visits, to measure web traffic, to offer you certain products or services, or to customize your visit. We use both session ID cookies and tracking cookies. Session cookies make it easier for you to navigate the Sites, and they expire when you close your browser. Tracking cookies help us understand how you use the Sites and enhance your user experience, and they remain on your hard drive for an extended period of time.

  Your Internet browser may include settings that permit you to block cookies or to be notified when cookies are placed. Please be aware that if you use these mechanisms to block or remove cookies, certain features and functions of the Sites may be unavailable or may not operate optimally.

- **Web Beacons** (also called "tracking pixels") are small graphic images, also known as "Internet tags" or "clear gifs" that are embedded in web pages and e-mail messages. Web beacons may be used for various purposes, such as to count the number of visitors to the Sites, to monitor how users interact with and navigate the Sites, or to verify how many articles or links were actually viewed.

- **Embedded Scripts** are designed to collect information about your interactions with the Sites. These scripts are temporarily downloaded onto your computer from our web server, or the server of a third party with whom we work. They are active only while you are connected to the Sites, and are deleted or deactivated thereafter.

Additional information about Tracking Technologies and your choices concerning their use are explained below in the Analytics Section and under Your Choices.

Information from Other Sources

We also may obtain information about you from other sources, such as other non-profit organizations, and combine that with information we collect about you. To the extent we combine such third-party sourced information with Personal Information we collect directly from you on the Sites, we will treat the combined information as Personal Information under this Privacy Policy. We are not responsible for the privacy statements or practices of third parties or on any other websites or online services that we do not control.

How we may use your information

We use information about you to operate the Sites and to deliver the content and services you request. In addition, we may use information about you for other lawful purposes, including to:

- Facilitate, manage, personalize and improve your online experience;
- Respond to your comments, questions and requests, provide customer service, send you informational notices, and contact you if we need to obtain or provide additional information;

- Conduct research and analysis, including focus groups and surveys about current services or of potential new services;
- Prevent and address fraud, breach of policies or terms, and threats or harm; and
- Send you advertisements and communicate with you regarding services, products, fundraising and events we think may interest you (for information about how to manage e-mail communications, see Your Choices below).

How we may share information

We may permit our agents, vendors, consultants, and other service providers to access information collected through the Sites to carry out work on our behalf. These third party service providers are prohibited from using Personal Information obtained in this manner for any purpose(s) other than to provide the services we have engaged them to perform. We also may share your information:

- To perform statistical analysis, send you e-mail or postal mail, or provide customer support;
- With our business partners, affiliates, and other third parties for purposes of sending their own marketing;
- With our affiliates for internal business purposes;
- If we are required to do so by law, regulation, or legal process (such as in response to a court order or subpoena);
- To fulfill requests by government agencies, such as law enforcement authorities;
- When we believe disclosure is necessary or appropriate to prevent physical harm or financial loss, or in connection with an investigation of suspected or actual illegal activity; or
- To enforce our policies, or protect rights, property, or safety.

If permitted by applicable law, we also may share your information in connection with, or during negotiations of, any proposed or actual merger, purchase, sale, or any other type of acquisition or business combination of all or any portion of our assets, or any transfer of all or a portion of our business to another company. We reserve the right to transfer any information we obtain through the Sites in the event we sell or transfer all or a portion of our business or assets (including in the event of a merger, reorganization, or liquidation).

Information you disclose publicly or to others

The Sites may include features, such as message boards, that allow you to freely submit information that can be viewed by others. We or others may store, display, reproduce, publish, distribute, or otherwise use such information (including the date and time you access the message board) in any media or format, and we may or may not attribute the content to you. Please keep in mind that if you post information on the Sites using these features, others have the ability to access and share that information with third parties.

Healthcare-related communications on message boards are not private and can be viewed by the community of cancer discussion participants who also use these features. MD Anderson is not responsible for the privacy, security, accuracy, use, or misuse of any information that you disclose, or that you receive from third parties, via message boards on the Sites.

Links to other websites

The Sites may include hyperlinks to other websites, online locations, platforms, or services for your convenience and information. Such linked websites may be operated by third parties that are not owned or controlled by MD Anderson. They may use their own cookies, web beacons, and other Tracking Technologies to collect information about you, and they may solicit Personal Information directly from you. If you follow links from the Sites to other websites, we encourage you to familiarize yourself with their privacy policies and terms of use. We are not responsible for the content or privacy practices of websites that we do not control.

Analytics services, advertising and online tracking

We may engage and work with third parties to serve advertisements on our behalf on the Sites or on other websites, and to provide analytics services about use of the Sites and performance of our ads and content on other websites. In addition, we may participate in online advertising networks and exchanges that display relevant advertisements to visitors, both on the Sites and on other websites, based on the visitors' interests as reflected by their browsing habits. Third parties may use cookies and other Tracking Technologies to automatically collect information about you and your activities, such as registering a unique identifier for your device and tying that to your online activities on and off of our Sites. We may use this information to analyze and track data, determine the popularity of certain content, deliver advertising and content targeted to your interests, and better understand your online activity.

Information about your use of the Sites and other websites may be collected using Tracking Technologies across time and services, and used for various purposes such as to associate different devices you use, and to deliver relevant and retargeted content, including interest-based ads.

Your web browser may have settings that allow you to transmit a "Do Not Track" signal when you visit various websites or use online services. Like many websites, the Sites are not designed to respond to "Do Not Track" signals received from browsers. To learn more about "Do Not Track" signals, click here.

Your choices

Accessing and Changing Information.

With few exceptions, you are entitled on your request to be informed about the information MD Anderson collects about you. Under Sections 552.021 and 552.023 of the Texas Government Code, you are entitled to receive and review the information. Under Section 559.004 of the Texas Government Code, you are entitled to have MD Anderson Cancer

Center correct information about you that is held by us and that is incorrect, in accordance with the procedures set forth in The University of Texas System Business Procedures Memorandum 32.

The information that MD Anderson Cancer Center collects will be retained and maintained as required by Texas records retention laws (Section 441.180 et seq. of the Texas Government Code) and rules. Different types of information are kept for different periods of time.

Communications

You can opt out of receiving promotional e-mails from us by clicking on the unsubscribe link in the email, or by changing your communication preferences when you log on to your account. Please note that your opt-out will not affect subsequent subscriptions or non-promotional communications from us, such as such as administrative and service announcements.

Tracking Technologies Generally

Regular cookies generally may be disabled or removed using tools available as part of most commercial browsers. In some instances, a browser may include settings that allow you to preemptively block cookies from being placed on your computer. Please be aware that if you disable or remove cookies and similar technologies, some parts of the Sites may not work properly. Also, if you revisit the Sites from a different computer or using a different browser, you may not be able to limit browser-based Tracking Technologies in the same way.

Analytics Services and Interest-Based Ads

The Sites use third-party web analytics services, such as Adobe Analytics and Google Analytics, to help us analyze how visitors use the Sites. For further information about Adobe Analytics and how they use analytics data, click here. To go directly to an opt-out tool for Adobe Analytics, click here. To learn more about opting out of data collection through Google Analytics, click here.

Often times, we may use certain advertising networks and exchanges that participate in the Network Advertising Initiative ("NAI"). NAI has developed a tool that allows consumers to opt out of certain interest-based advertising delivered by NAI members' ad networks. To learn more about opting out of such targeted advertising or to use the NAI tool, click here. Please be aware that such opt-outs do not affect non-targeted ads. We are not responsible for the effectiveness of, or compliance with, any third-parties' opt-out mechanisms or programs, or the accuracy of their statements regarding their programs.

Your California privacy rights

California's "Shine the Light" law permits customers in California to request certain details about how certain types of their information are shared with third parties and, in some cases, affiliates, for those third parties' and affiliates' own direct marketing purposes. Under this law, a business must either provide California customers certain information upon request, or permit California customers to opt-in to, or opt-out of, this type of sharing.

We may elect to share certain information about you that we have collected through the Sites with third parties for those third parties' direct marketing purposes. If you are a California resident, you may request information about our compliance with this law by emailing PrivacyCompliance@mdanderson.org or by sending a letter to the Chief Privacy Officer at The University of Texas MD Anderson Cancer Center, Institutional Compliance Office, Unit 1640, P.O. Box 301407, Houston, TX, 77230-1407. Requests must include "California Privacy Rights Request" in the first line of the description and include your name, street address, city, state, and zip code. Please note that we are only required to respond to one request per customer each year, and we are not required to respond to requests made by means other than through the e-mail address or postal mail address listed here.

Children's privacy

The Sites are not targeted to children under the age of thirteen (13). We do not knowingly collect personal information as defined by the U.S. Children's Privacy Protection Act ("COPPA") from children under 13, and if we learn that we have collected such information, we will delete it. If you are a parent or guardian and believe we have collected personal information from your child in a manner not permitted by COPPA, please contact us by emailing PrivacyCompliance@mdanderson.org.

Data security

We take reasonable measures to help protect personal information collected through the Sites from loss, theft, misuse, and other unauthorized access, disclosure, alteration, or destruction. Nevertheless, transmission via the Internet is not completely secure and we cannot guarantee the security of your information collected through our Sites.

Information for users outside the United States

MD Anderson is based in the U.S. and the information we collect is governed by U.S. law. If you are accessing the Sites from outside the U.S., please be aware that information collected through the Sites may be transferred to, processed, and stored in the U.S. Data protection laws in the U.S. may be different from those of your country of residence. Your use of the Sites, and providing information through the Sites, constitutes your consent to the transfer, processing, usage, sharing, and storage of your information, including Personal Information, in the U.S. as set forth in this Privacy Policy.

Changes to this Privacy Policy

We reserve the right to revise and reissue this Privacy Policy at any time. Any changes will be effective immediately upon posting of the revised Privacy Policy, and the new effective date will be listed at the top of this page. Subject to applicable law, your continued use of the Sites indicates your consent to the terms of the posted Privacy Policy. We encourage you to periodically review this Privacy Policy.

Contact us

If you have requests relating to your Personal Information, or if you have questions about this Privacy Policy, you may submit your questions online at https://www4.mdanderson.org/contact/ask-a-question/index.cfm, or contact us by emailing PrivacyCompliance@mdanderson.org, sending a letter to the Chief Privacy Officer at The University of Texas MD Anderson Cancer Center, Institutional Compliance Office, Unit 1640, P.O. Box 301407, Houston, TX, 77230-1407, or calling 1-877-632-6789.

EXHIBIT M

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: January 30, 2015

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, and is our terms of service that governs our relationship with users and others who interact with Facebook, as well as Facebook brands, products and services, which we call the "Facebook Services" or "Services". By using or accessing the Facebook Services, you agree to this Statement, as updated from time to time in accordance with Section 13 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

Because Facebook provides a wide range of Services, we may ask you to review and accept supplemental terms that apply to your interaction with a specific app, product, or service. To the extent those supplemental terms conflict with this SRR, the supplemental terms associated with the app, product, or service govern with respect to your use of such app, product or service to the extent of the conflict.

1. Privacy

Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.

2. Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Policy and Platform Page.)
4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use your feedback or suggestions without any obligation to compensate you for them (just as you have no obligation to offer them).

3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
10. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
11. You will not facilitate or encourage any violations of this Statement or our policies.

4. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.

10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. **Protecting Other People's Rights**

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or Trademarks or any confusingly similar marks, except as expressly permitted by our Brand Usage Guidelines or with our prior written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging and data charges, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

If you make a payment on Facebook, you agree to our Payments Terms unless it is stated that other terms apply.

8. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

If you are a developer or operator of a Platform application or website or if you use Social Plugins, you must comply with the Facebook Platform Policy.

9. **About Advertisements and Other Commercial Content Served or Enhanced by Facebook**

Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

10. **Special Provisions Applicable to Advertisers**

If you use our self-service advertising creation interfaces for creation, submission and/or delivery of any advertising or other commercial or sponsored activity or content (collectively, the "Self-Serve Ad Interfaces"), you agree to our Self-Serve Ad Terms. In addition, your advertising or other commercial or sponsored activity or content placed on Facebook or our publisher network will comply with our Advertising Policies.

11. **Special Provisions Applicable to Pages**

If you create or administer a Page on Facebook, or run a promotion or an offer from your Page, you agree to our Pages Terms.

12. **Special Provisions Applicable to Software**

1. If you download or use our software, such as a stand-alone software product, an app, or a browser plugin, you agree that from time to time, the software may download and install upgrades, updates and additional features from us in order to improve, enhance, and further develop the software.
2. You will not modify, create derivative works of, decompile, or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license, or we give you express written permission.

13. **Amendments**

1. We'll notify you before we make changes to these terms and give you the opportunity to review and comment on the revised terms before continuing to use our Services.
2. If we make changes to policies, guidelines or other terms referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.
3. Your continued use of the Facebook Services, following notice of the changes to our terms, policies or guidelines, constitutes your acceptance of our amended terms, policies or guidelines.

14. Termination

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 9.3, and 14-18.

15. Disputes

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions.
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, of any user of Facebook.
3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

16. Special Provisions Applicable to Users Outside the United States

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website. You will not use Facebook if you are prohibited from receiving products, services, or software originating from the United States.
3. Certain specific terms that apply only for German users are available here.

17. Definitions

1. By "Facebook" or" Facebook Services" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings; and (d) other media, brands, products, services, software (such as a toolbar), devices, or networks now existing or later developed. Facebook reserves the right to designate, in its sole discretion, that certain of our brands, products, or services are governed by separate terms and not this SRR.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post, provide or share using Facebook Services.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.
9. By "Trademarks" we mean the list of trademarks provided here.

18. Other

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.
10. We reserve all rights not expressly granted to you.
11. You will comply with all applicable laws when using or accessing Facebook.

By using or accessing Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy as amended from time to time. You may also want to review the following documents, which provide additional information about your use of Facebook:

- Payment Terms: These additional terms apply to all payments made on or through Facebook, unless it is stated that other terms apply.
- Platform Page: This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- Facebook Platform Policies: These guidelines outline the policies that apply to applications, including Connect sites.
- Advertising Policies: These guidelines outline the policies that apply to advertisements placed on Facebook.
- Self-Serve Ad Terms: These terms apply when you use the Self-Serve Ad Interfaces to create, submit, or deliver any advertising or other commercial or sponsored activity or content.
- Promotions Guidelines: These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- Facebook Brand Resources: These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- How to Report Claims of Intellectual Property Infringement
- Pages Terms: These guidelines apply to your use of Facebook Pages.
- Community Standards: These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

EXHIBIT N

Data Policy

Date of Last Revision: January 30, 2015

We give you the power to share as part of our mission to make the world more open and connected. This policy describes what information we collect and how it is used and shared. You can find additional tools and information at Privacy Basics.

As you review our policy, keep in mind that it applies to all Facebook brands, products and services that do not have a separate privacy policy or that link to this policy, which we call the "Facebook Services" or "Services."

I. What kinds of information do we collect?

Depending on which Services you use, we collect different kinds of information from or about you.

- **Things you do and information you provide.** We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.
- **Things others do and information they provide.** We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you, or upload, sync or import your contact information.
- **Your networks and connections.** We collect information about the people and groups you are connected to and how you interact with them, such as the people you communicate with the most or the groups you like to share with. We also collect contact information you provide if you upload, sync or import this information (such as an address book) from a device.
- **Information about payments.** If you use our Services for purchases or financial transactions (like when you buy something on Facebook, make a purchase in a game, or make a donation), we collect information about the purchase or transaction. This includes your payment information, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping and contact details.
- **Device information.** We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you've granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices. Here are some examples of the information we collect:
  - Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.
  - Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals.
  - Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.
- **Information from websites and apps that use our Services.** We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.
- **Information from third-party partners.** We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.
- **Facebook companies.** We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies. Learn more about these companies and their privacy policies.

II. How do we use this information?

We are passionate about creating engaging and customized experiences for people. We use all of the information we have to help us provide and support our Services. Here's how:

- **Provide, improve and develop Services.** We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services.

  We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friend tag you in a picture by comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged. If this feature is enabled for you, you can control whether we suggest that another user tag you in a photo using the "Timeline and Tagging" settings.

  When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby.

  We conduct surveys and research, test features in development, and analyze the information we have to evaluate and improve products and services, develop new products or features, and conduct audits and troubleshooting activities.

- **Communicate with you.** We use your information to send you marketing communications, communicate with you about our Services and let you know about our policies and terms. We also use your information to respond to you when you contact us.
- **Show and measure ads and services.** We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services. Learn more about advertising on our Services and how you can control how information about you is used to personalize the ads you see.
- **Promote safety and security.** We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies. We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning. We also offer easy-to-use security tools that add an extra layer of security to your account. For more information about promoting safety on Facebook, visit the Facebook Security Help Center.

We use cookies and similar technologies to provide and support our Services and each of the uses outlined and described in this section of our policy. Read our Cookie Policy to learn more.

III. How is this information shared?

Sharing On Our Services

People use our Services to connect and share with others. We make this possible by sharing your information in the following ways:

- **People you share and communicate with.**

  When you share and communicate using our Services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your Friends, or members of a Group. Likewise, when you use Messenger, you also choose the people you send photos to or message.

  Public information is any information you share with a public audience, as well as information in your Public Profile, or content you share on a Facebook Page or another public forum. Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV.

In some cases, people you share and communicate with may download or re-share this content with others on and off our Services. When you comment on another person's post or like their content on Facebook, that person decides the audience who can see your comment or like. If their audience is public, your comment will also be public.

- **People that see content others share about you.** Other people may use our Services to share content about you with the audience they choose. For example, people may share a photo of you, mention or tag you at a location in a post, or share information about you that you shared with them. If you have concerns with someone's post, social reporting is a way for people to quickly and easily ask for help from someone they trust. Learn More.
- **Apps, websites and third-party integrations on or using our Services.** When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.

  Learn more about how you can control the information about you that you or others share with these apps and websites.
- **Sharing within Facebook companies.** We share information we have about you within the family of companies that are part of Facebook. Learn more about our companies.
- **New owner.** If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.

Sharing With Third-Party Partners and Customers

We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.

Here are the types of third parties we can share information with about you:

- **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).** We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.

  Please review your advertising preferences to understand why you're seeing a particular ad on Facebook. You can adjust your ad preferences if you want to control and manage your ad experience on Facebook.
- **Vendors, service providers and other partners.** We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.

IV. How can I manage or delete information about me?

You can manage the content and information you share when you use Facebook through the Activity Log tool. You can also download information associated with your Facebook account through our Download Your Information tool.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.

You can delete your account any time. When you delete your account, we delete things you have posted, such as your photos and status updates. If you do not want to delete your account, but want to temporarily stop using Facebook, you may deactivate your account instead. To learn more about deactivating or deleting your account, click here. Keep in mind that information that others have shared about you is not part of your account and will not be deleted when you delete your account.

V. How do we respond to legal requests or prevent harm?

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm. For example, we may provide information to third-party partners about the reliability of your account to prevent fraud and abuse on and off of our Services. Information we receive about you, including financial transaction data related to purchases made with Facebook, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm. We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms.

VI. How our global services operate

Facebook, Inc. complies with the US-EU and US-Swiss Safe Harbor framework for the collection, use and retention of information from the European Union and Switzerland, as set out by the Department of Commerce. To view our certification, visit the Safe Harbor website.

As part of our participation in the Safe Harbor program, we will resolve disputes you have with us in connection with our policies and practices through TRUSTe. You can contact TRUSTe through their website.

Facebook may share information internally within our family of companies or with third parties for purposes described in this policy. Information collected within the European Economic Area ("EEA") may, for example, be transferred to countries outside of the EEA for the purposes as described in this policy.

VII. How will we notify you of changes to this policy?

We'll notify you before we make changes to this policy and give you the opportunity to review and comment on the revised policy before continuing to use our Services.

VIII. How to contact Facebook with questions

To learn more about how privacy works on Facebook, please check out Privacy Basics.

If you have questions about this policy, here's how you can reach us:

If you live in the US or Canada...

Please contact Facebook, Inc. online or by mail at:

Facebook, Inc.

1601 Willow Road
Menlo Park, CA 94025

If you live anywhere else...

The data controller responsible for your information is Facebook Ireland Ltd., which you can contact online or by mail at:

Facebook Ireland Ltd.
4 Grand Canal Square, Grand Canal Harbour
Dublin 2, Ireland

EXHIBIT O

Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel.law
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444
Fax: 310-854-0812

Barry. R. Eichen [Admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [Admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
Ashley A. Smith [Admitted *Pro Hac Vice*]
asmith@njadvocates.com
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

Stephen M. Gorny [Admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [Admitted *Pro Hac Vice*]
chris@gornylawfirm.com
THE GORNY LAW FIRM, LC
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

Jay Barnes [Admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [Admitted *Pro Hac Vice*]
rod.chapel@gmail.com
BARNES & ASSOCIATES
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

Attorneys for Plaintiffs

(Additional Attorneys Listed on Signature Page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WINSTON SMITH; JANE DOE I; and JANE DOE II, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.; AMERICAN CANCER SOCIETY, INC.; AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.; MELANOMA RESEARCH FOUNDATION; ADVENTIST HEALTH SYSTEM; BJC HEALTHCARE; CLEVELAND CLINIC; and UNIVERSITY OF TEXAS - MD ANDERSON CANCER CENTER,

Defendants.

CASE NO. 5:16-cv-01282-EJD

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Date: November 17, 2016
Time: 9:00 a.m.
Crtrm.: 4, 5th Floor
Judge: Hon. Edward J. Davila

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND CODES

RULES

TREATISES

I. INTRODUCTION

Privacy is not dead – not in sensitive health communications, not even on the Internet. Defendants' contentions to the contrary, the disclosure of personally-identifiable information ("PII") about persons communicating with health care providers over the Internet is not necessary for the Internet to function. The Mayo Clinic does not do it, nor does Johns Hopkins. The Defendants in this case do. That's what this case is about.

Far from "an attack on the way the Internet works," Plaintiffs instead seek to vindicate their constitutional, common law, and statutory rights to privacy in their sensitive medical communications with the health care Defendants who affirmatively (mis)represent that such communications are indeed private. In particular, this case is about: (1) the health care Defendants' websites' disclosure of sensitive medical communications to Facebook, in real-time, without the knowledge or consent of those with whom the Defendants are communicating (including their own patients), and in violation of their explicit privacy policies; and (2) Facebook's use of that sensitive information to sell targeted advertising.

Privacy is a fundamental right that finds its highest level of protection in medical information. *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998) ("One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]"); *see also*, *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) ("We deal with a right of privacy older than the Bill of Rights . . . .") Health privacy has also long been protected by the common law (*see DeMay v. Roberts*, 9 N.W. 146 (Mich. 1881)) and, in recent decades, by statute (*see, e.g.*, 42 U.S.C. § 1320d-6 (HIPAA); Cal. Civ. Code § 1798.91). In 2014, a unanimous Supreme Court held that Americans have a reasonable expectation of privacy in Internet medical communications – even when not made to a health care provider. *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("[C]ertain types of data are also qualitatively different. An Internet search and browsing history . . . could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

Facebook's self-serving argument to the contrary, general privacy principles still apply to the Internet. Although, as this Court has observed "this is an area of law that seems to be

developing," (*In re Facebook Internet Tracking Litig.*, Mot. to Dismiss Hr'g Tr. 17:12-13, Apr. 28, 2016) the trend is irrefutable – American courts in recent years have re-asserted and applied longstanding privacy rights to Internet communications – even outside the context of sensitive medical information. In *Google Cookie Placement*, the Third Circuit called defendants' argument that Internet tracking is "routine" and never highly offensive a "smokescreen" where the tracking at issue violated public privacy promises. 806 F.3d 125, 150 (3d Cir. 2015). Likewise, in *Nickelodeon Consumer Privacy Litig.*, the Third Circuit found plaintiffs adequately alleged a claim where the defendant "created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses." No. 15-1441, 2016 WL 3513782, at *22 (3d Cir. June 27, 2016). And in *Opperman v. Path*, the Court found that the unauthorized taking of consumer contact information was actionable, even over the defendants' objection that such behavior was "routine commercial behavior." 87 F. Supp. 3d 1018, 1058-61 (N.D. Cal. 2014).

Here, Defendants attempt a "universal defense"[1] to Internet privacy claims: if a company keeps its privacy policies vague but broad, nothing else matters – not their own promises, not legal prohibitions, and not sensitivity of information. According to Defendants, a broad statement buried in a privacy policy that no normal person ever reads (much less understands) creates immunity everywhere.[2] Taken to its logical conclusion, Facebook would be immune for its knowing receipt of, and profit from, hard copies of a person's complete medical file.

In effect, Facebook asserts obscure and vague privacy provisions operate as a blank check that must be read in isolation and trump any privacy policy on the health care Defendants' websites that expressly limits disclosure. Plaintiffs disagree and to find otherwise would be Orwellian. *See* George Orwell, *1984* 2 (1949) ("Big Brother is watching you . . . . The instrument (the telescreen, it

[1] *See In re: Facebook Internet Tracking Litig.*, Mot. to Dismiss Hr'g Tr. 30:7-9 ("THE COURT: It sounds like you're propounding a universal defense which is that's the way the Internet works, folks, and get over it.").

[2] *See Berkson v. GoGo, LLC*, 97 F. Supp. 3d 350, 381 (E.D.N.Y. 2015) (citing the comedian John Oliver, "If Apple put the entire text of Mein Kampf in their user agreement, you'd still click agree."); *see also Berkson* at 384 (citing a "[r]ecent empirical stud[y] analyzing the Internet browsing behavior of consumers" found that "between 0.05% and 0.22% of online shoppers access online agreements.").

was called) could be dimmed, but there was no way of shutting it off completely.").

Facebook and the health care Defendants are correct that the stakes are high. However, it is not the future of the Internet at stake but, rather, the future of Americans' fundamental right of privacy, which, once violated, can never be restored.

II. FACTUAL BACKGROUND AS ALLEGED[3]

The health care Defendants explicitly promise not to disclose PII to third-parties except in limited circumstances.[4] Facebook knows of these privacy promises.[5] The Plaintiffs sent and received sensitive medical communications with the health care Defendants.[6] However, in direct contravention of those privacy promises and without the knowledge or consent of the Plaintiffs, the health care Defendants disclosed PII about the Plaintiffs and details of their sensitive communications to Facebook in real-time.[7] What was promised to be kept private is no more. Significantly, disclosures to Facebook in violation of express privacy promises are not necessary to allow the health care Defendants' websites (or the Internet in general) to operate. In fact, Plaintiffs specifically alleged as much. Compl. ¶ 79 ("Facebook … does not track or intercept user

[3] As they have ignored the privacy of Plaintiffs and the Class, Defendants have also ignored that a Motion to Dismiss should address the allegations of the Complaint and no more. However, Defendants' Motion is replete with language that appears nowhere in the Complaint. *See, e.g.*, Mot. to Dismiss at 6:26–7:14 (touting, without citation, Defendants' reputations and work in a not-so-subtle attempt to excuse the conduct complained of).

[4] Compl. ¶¶ 107-12, Ex. F (Am. Cancer Soc.; "ACS"); 122-28, Ex. G (Am. Soc. of Clinical Oncology; "ASCO"); 137-43, Ex. H (Melanoma Research Foundation; "MRF"); 152-57, Ex. I (Adventist); 166-71, Ex. J (BJC); 181-84, Ex. K (Cleveland Clinic); 193-97, Ex. L (MD Anderson).

[5] Compl. ¶¶ 86-87, 129-31, 144-45, 158-59, 172-73, 185-86, 198-99, 222-24.

[6] Plaintiff Winston Smith sent and received communications relating to melanoma and cancer treatment. Compl. ¶¶ 117 (detailing communications with Cancer.org on treatment, insurance, support services, and lifestyle changes after cancer), 132 (detailing communications with Cancer.net on financing, treatment options, and emission tomography pet scans), 147 (detailing communications with Melanoma.org on baking soda treatment for melanoma), 202 (detailing communications with MDAnderson.org on metastatic melanoma). Plaintiff Jane Doe sent and received communications relating to pain management, treatment, and her doctor. Compl. ¶ 161 (detailing communications with ShawneeMission.org on pain management, orthopedic spine services, and Dr. Scott Ashcraft). Plaintiff Jane Doe II sent and received communications relating to a sensitive medical condition and her husband's doctor. Compl. ¶¶ 175 (detailing communications with BarnesJewish.org on her husband's doctor), 188 (detailing communications with ClevelandClinic.org on intestine transplants).

[7] Compl. ¶¶ 119-21 (ACS), 134-36 (ASCO), 149-51 (MRF), 163-65 (Adventist), 178-80 (BJC), 190-92 (Cleveland Clinic), 204-06 (MD Anderson).

communications with every website on which the Facebook icon appears. For example, … MayoClinic.org and … HopkinsMedicine.org include a small Facebook icon on nearly every page, but do not permit Facebook to track user communications. The same is true for hundreds if not thousands of other medical websites.").

Plaintiffs are members of Facebook who, like every other member, went through Facebook's sign-up process and agreed to its Terms, the first paragraph of which assures users:

> Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions. *Id.* at ¶ 60, Ex. A.

Despite underscoring that privacy is *very important* and promising to make *important disclosures*, Facebook fails to disclose that it tracks, collects, and intercepts user communications on sensitive health care websites in direct contravention of those websites' explicit privacy promises. *Id.* at ¶¶ 58-72. This interception occurs through the use of Facebook source code on web-pages controlled by the health care Defendants. As alleged, this code commandeers the Plaintiffs' web-browsers, permitting Facebook to acquire in real-time the communications connected to each user's IP address, browser fingerprint, and unique persistent Internet cookies assigned to each Facebook user and their particular browsers. *Id.* at ¶¶ 44-52.

Paragraph 50 illustrates how this works with an example of a communication between a user and Defendant ACS' Cancer.org website. *Id.* at ¶ 50a. First, the user sends the communication one of two ways – either by typing an entire URL into his web-browser toolbar, or by clicking on a hyperlink that contains information indicating it will send a communication on a particular topic – in this example, stomach cancer diagnosis. *Id.* at ¶ 50b. Regardless of whether the communication is sent manually by typing it into the toolbar or by a mouse click, the user has sent a communication to ACS about "stomach cancer diagnosis." *Id.* at ¶ 50c.

Immediately after the user hits Enter or clicks the mouse, the user's web-browser sends a GET request to ACS requesting information about stomach cancer diagnosis. *Id.* at ¶ 50d. However, unbeknownst to the user, the ACS webpage includes Facebook source code that directs the ACS web-server to commandeer the user's web-browser, ultimately commanding the browser to send a

separate but simultaneous GET request to Facebook attached to an exact duplicate of the user's communication to ACS. *Id.* at ¶ 50e. Without the user's knowledge, consent, or action, the web-browser follows commands from Facebook's source code, facilitating Facebook's real-time acquisition of (1) an exact copy of the communication the user sent to ACS, (2) cookie information that personally-identifies the user to Facebook, and (3) the user's IP address and device information, which also personally-identify the user to Facebook. *Id.* at ¶¶ 50f, 100-03. Facebook has acquired the communication and PII, but the communication between the user and ACS is still ongoing. *Id.* at ¶ 50f. ACS responds with a 2,535-word essay on stomach cancer diagnosis that does not finish loading until after Facebook acquired information about its substance. *Id.* at ¶ 50g.

In short, Facebook's code operates as an automatic routing program that permits Facebook to acquire exact duplicates of user communications, while they are still on-going, without the knowledge, consent, or any other action of the user. *Id.* at ¶ 52.

Much as it fails to disclose its activities to its users, Facebook also fails to disclose to web-developers that its source code as used by the health care Defendants will automatically result in Facebook's acquisition of communications.[8] *Id.* at ¶¶ 78, 84, Ex. D. After Facebook acquires the information, it uses it to sell advertisements targeted to users by medical conditions and interests including, but not limited to, lists such as "diabetes management," "chronic pain," "Hepatitis C," "bladder cancer," "rectal prolapse," and "diagnosis of HIV/AIDS." *Id.* at ¶¶ 88-91, Ex. E.

A. The Health Care Defendants' Privacy Policies

No reasonable person could read the health care Defendants' privacy promises and conclude that they disclose sensitive medical PII to Facebook in real-time.

American Cancer Society[9] – Defendants argue Cancer.org adequately informs users that it

[8] Without discovery, the plaintiffs cannot allege whether the health care Defendants knew about or consented to Facebook's acquisition of these sensitive communications in violation of their own privacy policies. *Id.* at ¶¶ 104-06.

[9] Cancer.org promises to "respect[] the privacy of every individual" who uses their websites. Comp. ¶ 109, Ex. F ("Because your privacy is important to us, we provide you with notice and choices about the collection and use of your information."). It next informs users that Cancer.org "use[s] cookies" but assures users that those cookies "do[] not contain any personal information." *Id.* at. Ex. F. It then promises that "Standard Web server traffic pattern information" on their websites "is shared externally only on an aggregated basis." *Id.* at. ¶ 110. ACS promises that user "health-related

discloses PII to Facebook via its advice to "read the privacy policies of each site you visit to determine what information that site may be collecting about you." Mot. to Dismiss 8:8-9. This is a non-sequitur – the PII disclosed by ACS is not occurring on another website, it is disclosed by ACS while the user is communicating with ACS. Defendants conveniently omit the rest of the paragraph:

> Our privacy policies apply only to your use of an ACS site. The www.cancer.org website contains links to other sites, including sites that have a special relationship with us. *We do not disclose personally identifiable information to those operating linked sites* and we are not responsible for their privacy practices. Links to other sites do not imply an endorsement of the materials or policies on those websites. You should read the privacy policies of each site you visit to determine what information that site may be collecting about you. Compl. Ex. F.

Thus, in addition to promising to only share traffic pattern information "on an aggregated basis," the very paragraph Defendants cite as notice includes another explicit promise: "We do not disclose personally identifiable information to those operating linked sites…." *Id.*

American Society of Clinical Oncology[10] – Defendants argue Plaintiffs are on notice of Cancer.net's PII disclosures to Facebook via a statement about "Click Stream Information." Mot. to Dismiss 8:1-7. Defendants again omit that the very sentence cited also refers to "Click Stream Information" as "NPI," defined one paragraph earlier as "anonymous Non-Personal Information." Compl. Ex. G § 4. As with Cancer.org, Defendants reference advice that users should "review the privacy policies of other sites carefully," but conveniently omit the rest of the paragraph. *Id*. at Ex. G. § 3 ("ASCO has also provided external links to other websites in order to provide those who use the Website with a better, more fulfilling experience. *Once you enter another website* … be aware that ASCO is not responsible for the privacy practices of other sites …. We encourage you to …

---

information is privileged and confidential and will not be shared or released to any organization or business entity other than those affiliated with or working in conjunction with ACS" as provided in specific examples. *Id.* at. ¶ 111, Ex. F.

[10] Cancer.net promises to "respect[] your privacy" and to be "committed to being transparent about how and when ASCO collects, uses, and safeguards the information we collect through our websites." Compl. Ex. G at 1. It then promises to tell users, among other things, "*who* collects information," "*what* information is collected and how this is done," and "*how* ASCO … discloses the information that is collected." *Id*. at Ex. G at 2. Despite this promise, ASCO does not disclose the *who* (the policy does not mention any relationship with Facebook), the *what* (it does not disclose the information Facebook collects), or the *how* (no mention of how it discloses information to Facebook). Instead, it promise to "only disclose your PII to third-parties" under a discrete list of seven circumstances, none of which were cited by Defendants or apply in this case.

review the privacy statements of each and every website that you visit through a link or sponsorship notice[.]") (emphasis added). Again, the disclosures are not happening on "another website" but rather this Defendant's own site.

Melanoma Research Foundation[11] – Defendants argue Plaintiffs are on notice of MRF's PII disclosures via a statement that "[m]any third-party sites have their own privacy policies that differ from ours." Mot. to Dismiss 8:10-11. Once again, Defendants omit the context:

> Our Service contains links to Internet sites maintained by third parties. These links are provided for your reference only. We do not control, operate or endorse in any respect information, products, or services on such third-party sites and are not responsible for their content. Many third-party sites have their own privacy policies that differ from ours. This Privacy Policy only covers our Service and does not cover any other site. Compl. Ex. H at ¶ 6.3.

Adventist[12] – Defendants argue Plaintiffs are on notice of Adventists' PII disclosures to Facebook via the "Links" section of its privacy policies. Mot. to Dismiss 8:11-13. Yet again, Defendants omit context:

> Our website may contain links to other sites. These links are for your convenience only, and Adventist Health System makes no representations or endorsements whatsoever regarding such other sites. You should review the privacy policies of other sites carefully before providing any information to such website. Adventist Health System is not responsible for the privacy policies or procedures or the content of any other website. Compl. Ex. I.

BJC Healthcare – Defendants argue Plaintiffs are on notice of PII disclosures to Facebook via a vague statement that "[i]nformation you submit may be routinely shared with … organizations working on [BJC's] behalf." Mot. to Dismiss 8:13-14. Again, Defendants omit the full context:

> A typical visit to our Web site does not require a user to submit personal information. However, if you decide to send us an email, respond to a survey, or subscribe to an online publication with your contact information, we will respond to you with the information you request and other information that we think might be of interest to you.…
>
> Information you submit may be routinely shared with our parent organization, BJC HealthCare as they often distribute our materials, or with the Washington University School of Medicine if you are looking for a physician referral. Other than these two organizations, we will only forward your personal information to

[11] MRF promises it does not "sell or share your Personal Data [defined as data that allows someone to identify or contact you] with Third Party Companies." Compl. Ex. H at ¶ 6.2.

[12] Adventist promises, "As a general rule, we will not disclose your personally identifiable information to any unaffiliated third party, except when we have your permission or under special circumstances[.]" Compl. Ex. I.

> organizations working on our behalf. We urge you not to provide any confidential information about you or your health to us via electronic communication. If you do so, it is at your own risk. Although we attempt to maintain our computer network in a secure manner to protect the content of your messages, we cannot provide absolute assurance that the contents of your email will not become accessible to individuals or entities that are not authorized to access your information. Compl. Ex. J at 2.

Thus, the language about "routine sharing" is limited to BJC itself and Washington University. Further, BJC's warning "not to provide any confidential information" is in the context of a disclaimer that BJC "cannot provide absolute assurance that the contents of your email will not become accessible" to unauthorized persons. Finally, Defendants' citation to a disclosure about BJC's own first-party cookies is completely irrelevant. First-party cookies are not at issue in this case.[13]

Cleveland Clinic[14] – Defendants argue Plaintiffs are on notice of Cleveland Clinic's PII disclosures to Facebook via statements about first-party cookies and disclaimers about site security. Mot. to Dismiss 8:18-20. Defendants' reference to first-party cookies is not relevant. Nor is the disclaimer. Defendants have again taken a sentence out of context. Just before the disclaimer, Cleveland Clinic provides the preface that, "[B]y its very nature, a website cannot be absolutely protected against intentional or malicious intrusion attempts." Compl. Ex. K at 2. While perhaps true, this Defendant could absolutely have taken steps to avoid the disclosure complained of here. Cleveland Clinic further professes that it will take "reasonable care to safeguard your information while in transit[.]" *Id*. at Ex. K at 3.

MD Anderson[15] – MD Anderson bases its defense solely on the Eleventh Amendment.

---

[13] Defendants neglect to mention that BarnesJewish.org does not maintain a clearly marked "Privacy Policy" link on its homepage. Instead, the bottom of each page includes a link to a "HIPAA" page, which assures users, "We are required by law to protect the privacy of your protected health information" and defines PHI to include "information that [BJC] create[s] or receive[s] that identifies you and your past, present or future health status or care[.]" Compl. ¶ 169, Ex. J. The Privacy Policy is only accessible through a link that states "Legal."

[14] ClevelandClinic.org promises, "Cleveland Clinic does not share any [PII] of any individual with any third party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization."

[15] MD Anderson promises, "Under no circumstances will we ever disclose (to a third party) personal information about individual medical conditions or interests, except when we believe in good faith that the law requires it." Compl. ¶197, Ex. L.

III. LEGAL STANDARDS

On a 12(b)(6) motion to dismiss, the Court must "accept factual allegations in the Complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine, Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). To survive, the complaint need only allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Dismissal is only appropriate "where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008).

IV. ARGUMENT

A. Plaintiffs Have Standing to Bring this Action

To establish standing under Article III, a plaintiff must allege that "he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo v. Robins*, 136 S. Ct. 1540, 1548 (2016).[16] "Concrete" is not synonymous with tangible and such harm may arise from a statutory violation. *Id.* at 1549 (citing cases involving fundamental rights to freedom of speech and religion as "intangible injuries" that "can nevertheless be concrete" and re-affirming that "Congress may elevate to the status of legally cognizable injuries, de facto injuries that were previously inadequate in law"). In such cases, *Spokeo* explains that a "right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified." *Id.*

1. Plaintiffs Allege Sufficient Privacy Harm

Where an alleged injury is intangible, *Spokeo* instructs courts to make two inquiries. First,

[16] Plaintiffs plead "particularized" injury. *See* Compl. ¶¶ 117, 132, 147, 161, 175, 188, 202.

"courts should consider 'whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing the basis for a lawsuit in English or American courts.'" *Mey v. Got Warranty*, No. 15-cv-00101-JPB-JES, 2016 WL 3645195 at *5 (N.D. W. Va. June 30, 2016) (citing *Spokeo*, 136 S. Ct. at 1548). "Second, Congress may 'elevate to the status of legally cognizable injuries that were previously inadequate at law.…' It 'has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.'" *Id.* at *6.

This case satisfies both inquiries: first, it involves the right to privacy, described by the Supreme Court as "a most fundamental human right" enshrined in the "specific guarantees in the Bill of Rights," "older than the Bill of Rights," and "the most comprehensive of rights and the right most valued by civilized men." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974); *Griswold*, 381 U.S. at 484; *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *accord*, *Berger v. New York*, 388 U.S. 41 (1967), citing 4 Blackstone Commentaries 168 (1765) and *Entick v. Carrington*, 19 How. St. Tr. 1029, 1066 (1765) ("Intrusions into privacy are 'subversive of all the comforts of society.'"). More specifically, privacy of a particularly sensitive sub-set of information invokes the highest standards of protection. *Norman-Bloodsaw* at 1269 ("One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health"). Since at least 1881, Americans have had standing to sue violators of their medical privacy even in the absence of economic harm. *See DeMay*, 9 N.W. at 146.

Post-*Spokeo* courts have found adequate standing allegations in privacy cases involving rights to privacy in information less substantial than medical communications. *See Bona Fide Conglomerate v. SourceAmerica*, No. 14-cv-00751-GPC-DHB, 2014 WL 4162020 (S.D. Cal. June 29, 2016) (stating that alleged violations of California Invasion of Privacy Act [also alleged in this case] satisfy *Spokeo*); *In re: Nickelodeon Privacy*, 2016 WL 3513782 at *6-8 (3d Cir. June 27, 2016) (finding standing based on alleged tracking and disclosure of minors' private personal information at the defendant's children's websites); *Mey v. Got Warranty*, Order Denying Defendants' Motion to Dismiss (finding standing under the Telephone Consumer Protection Act based on common law history of right to privacy and Congressional purposes in enacting the

TCPA).[17]

Second, this case involves precisely the type of harm Congress intended to prevent with the passage of the Electronic Communications Privacy Act of 1986. S. Rep. No. 99-541, at 5 (1986). "[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment . . . Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right . . . ." *Accord*, H.R. Rep. No. 99-647, at 19 (1986).

2. Plaintiffs Allege Sufficient Economic Harm

In addition to intangible but legally concrete privacy harm, Plaintiffs allege a robust market for the sensitive medical information wrongfully disclosed and tracked. Compl. ¶¶ 53-57 (describing "Value of the Personal Information Defendants Collect"), 88-91 (explaining how Facebook monetizes data wrongfully collected). This is enough. As Judge Koh recently explained in another medical privacy case, "Plaintiffs are not required to plead that there was a market for their PII and that they somehow also intended to sell their own PII." *In re: Anthem Data Breach Litig.*, No. 15-md-02617-LHK (N.D. Cal. May 27, 2016), Order Granting in Part and Denying in Part Defendants' Second Mot. to Dismiss, at *27. Instead, it is enough to allege "either an economic market for their PII or that it would be harder to sell their own PII, not both." *Id.* Likewise, Plaintiffs alleged "Benefit of the Bargain Losses" for Facebook's Breach of Fiduciary Duty of Good Faith and Fair Dealing. Compl. ¶ 362.

B. This Court Has Jurisdiction Over All of the Health Care Defendants

1. The Court's Exercise of Personal Jurisdiction Is Proper

A plaintiff need only make a prima facie showing of personal jurisdiction to withstand a motion to dismiss under Rule 12(b)(2). *Mattel, Inc. v. Greiner & Hausser GmbH*, 354 F.3d 857,

[17] Two cases cited by Defendant are inapposite. First, *Khan v. Children's National Health System* did not deal with the question of federal statutory standing as it involved plaintiffs' invocation of state-only data breach statutes in federal court. 2016 WL 2946165 (D. Md. May 19, 2016). Similarly, in *Gubala v. Time Warner*, plaintiffs alleged unlawful retention of information, not its unlawful collection or disclosure. 2016 WL 3390415 (E.D. Wis. June 17, 2016).

862 (9th Cir. 2003). Plaintiffs have alleged sufficient facts to support this Court's exercise of general and specific personal jurisdiction over the health care Defendants.

General Jurisdiction – A court may exercise general jurisdiction over foreign corporations to hear any and all claims against them when their affiliations with the State are so continuous and systematic as to render them essentially at home in the forum State. *Daimler AG v. Bauman*, 134 S. Ct. 746, 754 (2014). Contrary to Defendants' contention, the health care Defendants' affiliations with California are indisputably consistent and systematic and consist of significantly more than just operating a website. Indeed, the health care Defendants continuously and systematically send users' sensitive medical communications to Facebook, which is headquartered in California, each and every time a user sends a GET request to the health care Defendants' respective websites. Such activity is not random or fortuitous. It is nothing less than continuous and systematic, thereby rendering them essentially at home in California and subject to this Court's general jurisdiction.

Specific Jurisdiction – A defendant is subject to specific jurisdiction if (1) it purposefully directed its activities to the forum or purposefully availed itself of the privilege of conducting activities in the forum, (2) the plaintiff's claim arises out of the defendant's forum-related activities, and (3) the exercise of jurisdiction comports with fair play and substantial justice, that is, it is reasonable. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004).

Here, all three prongs of the specific jurisdiction test are satisfied. First, the health care Defendants purposefully directed their activities to California. That Plaintiffs do not reside in California is not fatal. *See Walden v. Fiore*, 134 S. Ct. 1115, 1122 (2014). As explained above, the health care Defendants send users' sensitive medical communications to Facebook every time a user sends a GET request to the health care Defendants' respective websites. Additionally, such Defendants seemingly concede that their conduct is purposeful in that, in their Motion, they contend that their respective websites sufficiently disclosed such conduct. Mot. to Dismiss 7:20-26, 18:5-13.

Second, Plaintiffs' claims clearly arise out of the health care Defendants' California-related activities. Namely, Plaintiffs' claims arise out of, in substantial part, the health care Defendants' sending Plaintiffs' sensitive medical communications to Facebook in real-time, without Plaintiffs' knowledge or consent, and in violation of the health care Defendants' explicit privacy promises.

Third, this Court's exercise of jurisdiction over the health care Defendants comports with fair play and substantial justice. The fulcrum of activity in this action is with Facebook. The health care Defendants' relevant conduct occurred in California. Additionally, pursuant to Facebook's Terms of Service, Facebook users, including web developers and operators like the health care Defendants, submit to this Court's personal jurisdiction for the purpose of litigating all claims related to Facebook. Compl. Ex. A at 4. This Court is the single most reasonable court in which Plaintiffs could bring this action against the health care Defendants.

ACS's argument that its Georgia forum selection clause prevents this Court from exercising personal jurisdiction over it is also without merit. To the contrary, each health care Defendant, including ACS, is subject to Facebook's forum selection clause and this Court's jurisdiction since non-parties can be held to forum selection clauses if the conduct of the non-parties is closely related to the contractual relationship. *Manetti-Farrow, Inc. v. Gucci America, Inc.*, 858 F.2d 509, 514 n.5 (9th Cir. 1988); *Holland Am. Line, Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 456 (9th Cir. 2007). The health care Defendants' relevant conduct is inextricably related to the relationship between Plaintiffs and Facebook. Moreover, this claim stems from users like Plaintiffs being Facebook members and the health care Defendants being users of Facebook code. The health care Defendants, therefore, are subject to Facebook's forum selection clause and this Court's jurisdiction.

2. MD Anderson Is Not Immune from Suit

Under the Full Faith and Credit Clause, the law demands application of California's typical rules of immunity and California's immunity-related statutes. *See Franchise Tax Bd. of Cal. v. Hyatt*, 136 S. Ct. 1277, 1281-82 (2016); *Nevada v. Hall*, 440 U.S. 410, 424 (1979) (California court may apply California sovereign immunity law to State of Nevada). MD Anderson may only rely on sovereign immunity, if at all, to the extent consistent with California law. *Hyatt*, 136 S. Ct. at 1281-82. The California state-law claims should not be dismissed as the allegations are sufficient to state claims against MD Anderson under California law. Further, as discussed above, MD Anderson, by using Facebook's code, affirmatively consented to California law and chose California as the venue for disputes. Additionally, the Wiretap Act permits an aggrieved party to sue "the person *or entity*, other than the United States, which engaged in that violation." 18 U.S.C. § 2520(a) (emphasis

added). *Seitz v. City of Elgin* explicitly forecloses Defendants' argument: "the plain meaning of 'entity' includes government units." 719 F.3d 654, 657 (7th Cir. 2013). Thus, any purported sovereign immunity is explicitly waived in the Wiretap Act. 18 U.S.C. § 2520(a).

C. Plaintiffs' Claims Survive Dismissal

1. Plaintiffs Did Not Consent to the Harm Complained of

Defendants bear the burden of proving the affirmative defense of consent. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003). However, as consent does not appear in the Complaint, it should not be resolved on Facebook's 12(b)(6) motion. *Scott v. Kuhlmann*, 746 F.2d 1377-78 (9th Cir. 1984) (citing Wright & Miller, Federal Practice and Procedure § 1277 at 328-30) (affirmative defenses ordinarily may not be raised in motion to dismiss unless there are no disputed issues of fact); *Conway v. Geithner*, No. C-12-0264, 2012 WL 1657156 at *2 (N.D. Cal. 2012). Accordingly, Defendants have not carried their burden.

a. Consent for Sensitive Medical Information Must Be Express, Knowing, and Written

This is not a case about the disclosure of ordinary information, but instead sensitive medical information, which is afforded the highest degree of constitutional, common law, and statutory protection from tracking and disclosure. Compl. ¶ 216b ("The Plaintiffs' communications with Adventist, BJC, Cleveland Clinic, and MD Anderson related to their 'past, present, and future physical or mental health or condition.'"). To rule on this Motion, this Court will necessarily have to apply a test to determine whether the Defendants' disclosures were adequate and that Plaintiffs consented to the challenged activity. The proper tests for tracking and disclosure of sensitive medical information are found in HIPAA and California Civil Code section 1798.91. Under these tests (or as detailed below, the test urged by Defendants), Plaintiffs have not consented.

HIPAA – Disclosure and receipt of medical information requires express, knowing, and written consent. "A person who knowingly and in violation of [HIPAA] – (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section." 42 U.S.C. § 1320d-6(a). "[A] person . . .

shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." *Id.*

Defendants Adventist, BJC, Cleveland Clinic, and MD Anderson are "covered entities" under HIPAA. Defendants argue, however, that they are only "covered entities" when engaged in "specific transactions." Mot. to Dismiss 28:13-29:3. This argument is at odds with the plain language of 42 U.S.C. § 1320d-6(a) cited above, as well as the regulations enforcing HIPAA. Under 45 C.F.R. § 164.502, a "covered entity … may not use or disclose protected health information, except as permitted or required [by HIPAA]." This requirement is not limited to the instances when a covered entity is engaged in one of the "specific transactions" cited by Defendants. For example, covered entities were found to violate HIPAA by (1) leaving a telephone message on a patient's answering machine,[18] and (2) responding to a subpoena without making reasonable efforts to ensure that the individual whose PII was sought had received notice of the request.[19] Neither of these HIPAA violations involved one of the "specific transactions" referenced by Defendants.

In addition, "protected health information," by the plain language of the Privacy Rule, is not limited to patients of a covered entity. Instead, "health information" is defined as "any information … whether oral or recorded in any form or medium that … (1) is created or received by a health care provider … and (2) [r]elates to the past, present, or future physical or mental health or condition of an individual." 45 C.F.R. § 160.103. "Health information" becomes "protected" under HIPAA when it is "individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form of media." 45

[18] "Large Provider Revises Contact Process to Reflect Requests for Confidential Communications," U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case2; "Hospital Implements New Minimum Necessary Policies for Telephone Messages," U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case26.

[19] "Public Hospital Corrects Impermissible Disclosure of PHI in Response to a Subpoena," U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case9.

C.F.R. § 160.103. In turn, information is considered "individually identifiable" under HIPAA unless it has been scrubbed of all "identifiers of the individual *or* of *relatives*, employers, or *household members* of the individual." 45 C.F.R. § 164.514(b)(2) (emphasis added). These "identifiers" include names, geographic subdivisions smaller than a state, device identifiers and serial numbers, IP addresses, and any other unique identifying numbers, characteristics or code tied to "the individual" or their "relatives, employers, or household members." 45 C.F.R. § 164.514(b)(2).

Information considered PII may only be disclosed with proper HIPAA authorization on a signed document containing (1) "specific and meaningful" disclosures of the information to be disclosed, (2) the persons to whom it will be disclosed, a description of the information to be disclosed, (3) an expiration date for disclosure, and (4) notice of the right to revoke authorization. Compl. ¶ 212. The covered entity must also write its authorization in plain language and provide the individual with a signed copy. *Id.*

In this case, the Plaintiffs' communications are protected by HIPAA. The communications at issue were recorded and received by health care providers. *Id.* at ¶ 215 ("the covered entity websites each tracked, created, and recorded logs of the Plaintiffs' activities on the health care websites through the websites' own use of cookies and other [PII] including, but not limited to, device identifiers and IP addresses."). These communications relate to the Plaintiffs' "past, present, or future physical or mental health or conditions," or, in the case of Jane Doe II, her spouse. *Id.* at ¶¶ 216b ("The Plaintiffs' communications with Adventist, BJC, Cleveland Clinic, and MD Anderson related to their 'past, present, and future physical or mental health or condition.'"), 161 ("Plaintiff Jane Doe sought information … relating to pain management and her particular doctor."), 175 ("Plaintiff Jane Doe II sought information … relating to a sensitive medical condition, and her husband's doctor.").[20] The communications were disclosed to Facebook connected to information deemed individually-identifiable under 45 C.F.R. § 164.514(b)(2). *Id.* at

[20] To the extent necessary, Plaintiffs will if given leave, file an amended complaint alleging that Plaintiff Winston Smith was also seeking information and engaging in communications relating to his own "past, present, and future physical or mental health or conditions."

¶¶ 82 (describing Facebook cookies), 99-103 (describing why even non-cookie information (IP addresses and device identifiers) are personally identifiable to Facebook), 220. Finally, the covered entities disclosed the information to Facebook in the absence of a valid HIPAA authorization – and, in fact, in direct violation of their own privacy policies. *Id.* at ¶ 221.

Cal. Civ. Code § 1798.91 – California law provides that "[a] business may not request in writing medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share or otherwise disclose that information for direct marketing purposes" unless it first "disclose[s] in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual" and "obtain[s] the written consent of the individual to whom the information pertains … to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual." Cal. Civ. Code § 1798.91. Facebook is a business engaged in direct marketing. Compl. ¶¶ 227-28. Plaintiffs' communications qualify as "medical information" under this section. *Id.* at ¶ 230. Facebook's disclosures were not "clear and conspicuous." *Id.* at ¶¶ 233-34.

b. ECPA Consent Must Be "Actual" and Not "Casually Inferred"

For ECPA claims, "consent should not casually be inferred." *Pharmatrak* at 20. "Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception." *Id*. "Consent may be explicit or implied, but it must be actual consent rather than constructive consent." *Id*. at 19. It involves a two-part inquiry. First, a court must determine the "dimensions of the consent." *Id*. Then, it must ascertain "whether the interception exceeded those boundaries." *Id.*[21]

In *Pharmatrak*, the defendant was a third-party cookie company whose source code was voluntarily placed onto the websites of health care (pharmaceutical) companies. Even though the health care websites placed Pharmatrak code on their webpages, they did not know of or consent to the extent of the information Pharmatrak acquired. The Court found the plaintiffs provided adequate

[21] This analysis is no different in the Internet context than in any other. A medical patient may consent to one treatment (a physical exam), but refuse another (colonoscopy). A landowner may consent to one trespass (bird-watching), but not another (duck hunting).

evidence to assert an ECPA claim. As in *Pharmatrak*, this case involves third-party cookies utilized through source code on a health care company's website. And, each health care Defendant explicitly promised not to disclose certain information to Facebook, even though it did (discovery will reveal the extent of the health care Defendants' knowledge of and consent to Facebook's activities). Further, "[t]he existence of implied consent is a question of fact[.]" *Konop v. Hawaiian Airlines, Inc*., 236 F.3d 1035, 1047-48 (9th Cir. 2001) (citing *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990) ("The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of [the Wiretap Act] – a purpose which suggests that consent should not casually be inferred.")).

Defendants assert that the test for consent in this case is: "Would a reasonable user who viewed [the defendants'] disclosures have understood that [Facebook] was collecting [the information at issue]?" Mot. to Dismiss 16:7-8, citing *Perkins v. LinkedIn Corp*., 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014). But, in light of HIPAA and California Civil Code section 1798.91's greater protections for sensitive medical information, this misstates the question. It also leaves out half of the equation: would a reasonable user have understood that the health care Defendants were disclosing personally identifiable information about them to Facebook even though their privacy policies explicitly promised not to share such information?

Regardless, even under Defendants' test, a reasonable user would not have understood that the health care Defendants were violating their own privacy policies. *Perkins* explains why. There, LinkedIn's disclosure "was not, as is often the case, … buried in a Terms of Service or Privacy Policy that may never be viewed or if viewed at all on a wholly separate page disconnected from the processes that led to the alleged wrongful conduct." *Perkins*, 53 F. Supp. 3d at 1212. "Even more significantly, perhaps," *Perkins* explains, "is the fact that alongside the disclosure is an express opt out opportunity in the form of the 'No thanks' button." *Id. Perkins* determined it was only "[i]n light of the clarity of the disclosure, the proximity of the disclosure to the wrongful conduct, and the ability to opt out" that the LinkedIn plaintiffs consented to and authorized the

collection of email contacts. *Id.* Here, however, (1) the health care Defendant explicitly promised not to disclose PII, Facebook failed to disclose that it collects PII in this way, and any Facebook disclosures were vague and contained in a Privacy Policy "on a wholly separate page;" (2) the wrongful conduct occurred on the webpages of health care Defendants far away from the vague disclosure "buried in a Terms of Service or Privacy Policy that may never be viewed;" and (3) Facebook users do not have the option to opt-out of Facebook's tracking of this medical information.

Review of the health care Defendants' privacy policies in light of the particular sections cited in the Motion demonstrates that no reasonable person would have understood that their websites were disclosing PII to Facebook. As explained above, Defendants offer a series of non-sequiturs regarding the explicit promises made by the health care Defendants. Further, Facebook's Statement of Rights and Responsibilities ("SRR") combined with its Data Use Policy cannot be said to apprise reasonable persons that Facebook would track their sensitive medical communications with websites that explicitly promise not to make such disclosures. Again, Facebook's SRR begins by promising users, "Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information." Compl. ¶ 60, Ex. A ¶ 1 (emphasis added). Is a disclosure that Facebook tracks, records, and intercepts sensitive medical communications that its users make on health care websites' (including HIPAA-covered entities) that explicitly promise not to disclose the contents of those communications *important*? A reasonable person would believe it was, and yet Facebook made no such disclosure.

To the extent Facebook has disclosed anything with regard to its tracking and acquisition of communications, applying those disclosures to communications the Plaintiffs exchanged with the health care Defendants in this case would render Facebook's SRR and Data Use Policy unenforceable and unconscionable. Defendants argue these vague but broad terms create a universal defense to all privacy actions. Yet, just as ordinary privacy and consent principles apply to the Internet, so too do ordinary contract principles. *See Specht v. Netscape*, 306 F.3d 17, 30 (2d Cir. 2002) (J. Sotomayor) (interpreting California contract law as it applied to Internet Terms of Use,

"California's common law is clear that 'an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious."); *Berkson*, 97 F. Supp. 3d at 404 (discussing procedural and substantive unconscionability in Internet contracts of adhesion, citing Restatement (Second) of Contracts § 211(3), where the offering party has reason to believe "that the party manifesting assent" to a contract "would not do so" if she "knew that the writing contained a particular term, the term is not part of the agreement"); *Mastrobuono v. Shearson Lehman Hutton, Inc.*, 514 U.S. 52, 63 (1995) ("As a practical matter, it seems unlikely that petitioners … had any idea that by signing a standard-form agreement to arbitrate disputes they might be giving up an important substantive right. In the face of such doubt, we are unwilling to impute this intent to petitioners.").

2. The Wiretap Act Claim Is Proper

Interception – The ECPA defines "intercept" as the "acquisition of the contents of any … electronic communication[.]" Federal courts have squarely rejected Facebook's argument that the acquisition must be made via the same communication. In language directly on point, the First Circuit rejected an identical argument with respect to a third-party cookie defendant's acquisition of the content of sensitive medical information on health care websites:

> Even those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception. … NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third-party (Pharmatrak).
>
> Pharmatrak argues that there was no interception because 'there were always two separate communications: one between the Web user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak.' This argument fails
>
> for two reasons. First, as a matter of law, even the circuits adopting a narrow reading of the Wiretap Act merely require that the acquisition occur at the same time as the transmission; they do not require that the acquisition somehow constitute the same communication as the transmission. Second, Pharmatrak acquired the same URL query string (sometimes containing personal information) exchanged as part of the communication between the pharmaceutical client and the user. Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement.

In re: Pharmatrak, 329 F.3d at 22; *see also U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010)

(email forwarding).

Facebook also attempts to shoehorn the Wiretap Act's exception for a "party to the communication" into its "interception" defense. However, as this Court has previously held, Facebook cannot claim the "party" exemption simply because a "Facebook server was involved" when there is nothing to "demonstrate that Plaintiffs knew that fact while their browsing activity was being tracked and collected." *In re: Facebook Internet Tracking Litig.*, Order Granting Def.'s Mot. to Dismiss at 18. Also, Defendants' reliance upon the "party to the communication" rule stated in *Google* and *Nickelodeon* is misplaced. In *U.S. v. Eady*, decided in the five months between those cases, the Third Circuit adopted a different rule, defining "party to the communication" as "an individual who participates with at least one other individual in a communication and whose participation in that communication is known to the other participant(s) in the communication at the time of the communication." 2016 WL 2343212 (3d Cir. May 4, 2016) (unpublished opinion). As the *Eady* panel explained, "a defendant does not actually participate in a conversation unless his presence is known to the other participants." *Id*. at *3.

In this case, Plaintiffs did not know Facebook was acquiring the communications they were exchanging with the health care Defendants. And, as set out above, the health care Defendants explicitly promised the opposite. In addition, Facebook did not disclose to its users that it acquires their communications with the health care Defendants nor that it acquires communications in violation of other websites' privacy policies or federal and state medical and other privacy laws.

Content – Under the Wiretap Act, content "includes any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The Complaint details 15 instances in which Facebook acquired information concerning the substance, purport, or meaning of a communication. Compl. ¶¶ 117, 132, 147, 161, 175, 188, 202, 269. For example, Facebook acquired communications between Winston Smith and MD Anderson relating to "Metastatic Melanoma" via: http://www2.mdanderson.org/cancerwise/2012/06/metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis.html. Id. at ¶¶ 202, 269(g). The phrase "metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis" includes information concerning the "substance, purport, and meaning" of the communications between Winston Smith

and MD Anderson. Arguments to the contrary are absurd.

No court has ever ruled that URLs as specific as these are not protected by the Wiretap Act. In *Zynga*, the Ninth Circuit explained that URLs contain content where they include "search term[s] or similar communication[s] made by the user[.]" *In re: Zynga Privacy*, 750 F.3d 1098, 1109 (9th Cir. 2014). In *Google Cookie*, the Third Circuit explained "post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user … between the information revealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that – at a minimum – some queried URLs qualify as content." *In re: Google Cookie Placement*, 806 F.3d at 139. As this Court has noted, the *Google Cookie* Court's "analysis of this type of communication" was "very thorough … impressive … and very thoughtful" and what *Google Cookie* "tells us [is] that there are other circumstances when you drill down, not necessarily that deep, that you can find that the URLs have actual content and ours could be offensive in some manner." *See In re: Facebook Internet Tracking Litig.*, Mot. to Dismiss Hr'g Tr. 17-18.

This is one of those circumstances. Case law, legislative history, and logic on this point overwhelmingly support the Plaintiffs. *See U.S. v. Forrester*, 512 F.3d 500, n.6 (9th Cir. 2008) (URLs, unlike mere IP addresses, "reveal[] much more information" about user's activity, including articles viewed); *Declassified Opinion from the FISC*, https://www.dni.gov/files/documents/1118 CLEANEDPRTT%202.pdf (content and DRAS under ECPA not mutually exclusive); *In re: Application for Pen Register*, 396 F. Supp. 2d 45, 49-50 (D. Mass. 2005) ("Contents" include URL "subject lines, application commands, search queries, requested file names, and file paths); *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000) (post-dialed digits); *Brown v. Waddell*, 50 F.3d 285, 87-88 (4th Cir. 1995); *In re: Pharmatrak*, 329 F.3d at 18; H.R. Rep. 107-236, at 53, 294-96 (2001) (legislative history to PATRIOT ACT, explaining a pen register order "could not be used to collect information other than [DRAS], such as the portion of a URL specifying Web search terms or the name of a requested file or article" and that, according to Rep. Zoe Lofgren (D-San Jose), "in the discussions that we had … with the Justice Department and the White House, they made it very clear that they agreed with this, and this is not an agreement. It is just a clarification,

and I think that is important for the public to know[.])[22]

Device – The ECPA defines an "electronic … or *other* device" as "*any* device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). "Other" and "any" focus the ECPA definition on function – *i.e.*, whether something can be used to intercept (acquire) communications. Congress chose broad definitions to further the central purpose of the Wiretap Act – "to protect effectively the privacy of … communications." *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001). The dictionary definition of device includes, among other things, (1) "a thing made for a particular purpose; an invention or contrivance"; (2) "a plan or scheme for effecting a purpose," and (3) "a crafty scheme, trick." http://www.dictionary.com/browse/device.

Plaintiffs allege seven different devices: (1) cookies and other tools used by Facebook to track Plaintiffs' communications; (2) the Plaintiffs' web-browsers; (3) the Plaintiffs' computing devices; (4) Facebook's web servers; (5) the web servers of the health care Defendants; (6) the source code deployed by Facebook to effectuate its acquisition of communications; and (7) the plan Facebook carried out to effectuate the acquisition of information in this case. Compl. ¶ 261; *see also Id*. at ¶ 50 (describing how these devices work together to effectuate Facebook's scheme).

Web servers and computers are devices under the ECPA.[23] *Szymuszkiewicz*, 622 F.3d at 707 (discussing *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001)). Software and computer code are devices. *In re: Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1067 (N.D. Cal. 2015). Facebook's cookies are ECPA devices because they are an invention

---

[22] The full report is available online through the United States Government Printing Office. *See* https://www.congress.gov/107/crpt/hrpt236/CRPT-107hrpt236-pt1.pdf

[23] *Crowley* and *Potter* cited by Defendants are inapposite. In *Crowley*, the Court held that Amazon could not be liable because it "acted as no more than a second party to a communication" when it knowingly forwarded information to a credit card verification company. 166 F. Supp. 2d 1263, 1266 (N.D. Cal. 2001). In *Potter v. Havlicek*, the Court concluded that "computer software alone" is not a "device" because the ECPA "does not contemplate imposing civil liability on software manufacturers and distributors for the activities of third parties" in a case arising out of a nasty divorce where the victim of a jealous husband sued the husband for a Wiretap violation and the husband interpleaded the company that designed the software he used to spy on his spouse. 2008 WL 2556723 at *7 (S.D. Ohio June 23, 2008). Plaintiffs here allege seven devices, not computer software alone. More importantly, the Defendants are not arms-length software designers but instead the actual acquirers of the Plaintiffs' communications.

"designed to track and record an individual Internet user's communications … across the Internet." Compl. ¶ 41.

Criminal or Tortious Purpose – Defendants may be liable under the ECPA even if they have the consent of a party to the communication or are deemed a party to the communication where "such communication is intercepted [i.e. acquired] for the purpose of committing any criminal or tortious act in violation of … the laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). In *Sussman v. ABC*, the Ninth Circuit explained this statutory exception to the consent and party exceptions applies where the underlying act is criminal or tortious for reasons unrelated to the means by which it was carried out. 186 F.3d 1200 (9th Cir. 1999). "Under §2511, the focus is not upon whether the interception violated another law; it is upon whether the purpose for the interception – *its intended use* – was criminal or tortious. … Where the taping is legal, but is done for the purpose of facilitating some further impropriety … section 2511 applies." *Id*. at 1202.

In this case, the precise method by which Facebook acquired and the health care Defendants disclosed PII is not the entire harm. Suppose Defendants had carried out this scheme without the use of the Internet – rather than disclosing PII via cookies, IP addresses, and device identifiers, the health care Defendants mailed Facebook a hard-copy database of every person with whom they exchanged off-line communications regarding medical conditions, services, or providers.[24] After receiving this information off-line, Facebook uses it for advertising. As they do in this case, the plaintiffs in such a situation would have actionable claims, and the defendants' conduct would violate several other medical privacy laws. Here, it is not just that Defendants schemed to acquire and disclose the Plaintiffs' communications in real-time without authorization. The nature of the information exchanged makes it tortious because the unauthorized acquisition and disclosure of sensitive health information is criminal and tortious – regardless of the technology employed.

3. Plaintiffs State a Claim Under the California Invasion of Privacy Act

CIPA § 631 – Plaintiffs re-state the arguments made for the federal Wiretap claim regarding

[24] This hypothetical is not far-fetched. *See* http://adage.com/article/datadriven-marketing/marketers-board-offline-online-data-train/293220/ (describing how Facebook and other companies are working to "turn[] offline consumer data into a tool for digital marketing.").

"content," Facebook's status as a "third-party" cookie company outside the Wiretap Act's exception for parties to a communication, and "device." In addition, Plaintiffs point this Court to the actual text of CIPA, which does not require a "device" but instead prohibits interceptions "by means of any machine, instrument, or contrivance, *or in any other manner*" (emphasis added). Like the federal Act, CIPA focuses on function, not static form.

CIPA § 632 – Plaintiffs plead CIPA section 632 in the alternative. If Facebook is deemed a party to the communication even though it is admittedly a "third-party cookie" company, CIPA section 632 also forbids recording a conversation where "a party to [the] conversation has an objectively reasonable expectation of privacy that the conversation is not being overheard or recorded," *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). As Facebook duly notes, California courts have held that Internet communications cannot be considered confidential in some circumstances. Mot. to Dismiss 23:15-17. However, no California court has held that an Internet communication is not confidential when one of the parties to the communication explicitly promises that it will not be disclosed to a third-party. In *Nickelodeon*, the Third Circuit ruled that a website's privacy promises may "create[] an expectation of privacy" on those websites. No. 15-1441, 2016 WL 3513782, at *22 (3d Cir. June 27, 2016). In this case, the health care Defendants not only "created an expectation of privacy" by their very promises but that expectation was made all the more reasonable by the fact that the health care Defendants are HIPAA-covered entities or otherwise trusted health care organizations, and that "[o]ne can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]" *Norman-Bloodsaw*, 135 F.3d at 1269. Facebook's assertion that CIPA "was intended to apply to traditional recording mechanisms" and not Internet technology flies in the face of California courts' consistent modernizing of CIPA. *See In re: Google Inc. Gmail Litig.*, 2013 WL 5423918 at *21 (N.D. Cal. 2013) (noting California Supreme Court has consistently interpreted CIPA broadly and "regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme.").

Pre-emption – The Wiretap Act does not pre-empt CIPA or other state laws (including common law claims) designed to protect privacy. *See Shively v. Carrier IQ*, No. C-11-5775 EMC,

2012 WL 3026553, at *3-5 (N.D. Cal. July 24, 2012); *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011); *In re: NSA Telcomms. Records Litig.*, 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007); *Leong v. Carrier IQ*, No. 12-01562 GAF (MRWx), 2012 WL 1463313 (C.D. Cal. Apr. 27, 2012); *Lane v. CBS Broad., Inc*., 612 F. Supp. 2d 623, 637 (E.D. Pa. 2009); *People v. Conklin*, 12 Cal. 3d 259 (1974); *Kearney v. Solomon Smith Barney, Inc*., 39 Cal. 4th 95 (2006). "Complete preemption … arises only in 'extraordinary' situations. The test is whether Congress clearly manifested an intent to convert state law claims into federal-question claims." *Ansley v. Ameriquest Mortg. Co*., 340 F.3d 858, 862 (9th Cir. 2003).

In *Shively v. Carrier IQ*, Judge Chen noted "*Bunnell* is fundamentally flawed because it fails to take into account the legislative history[.]" *Shively*, No. C-11-5775 EMC, 2012 WL 3026553 at *5. The legislative history to the Wiretap Act makes clear that Congress did not intend to supplant state law. *See* S. Rep. No. 90-1097, at 2187 (1968) ("The proposed provision envisions that *States would be free to adopt more restrictive legislation*, or no legislation at all, but not less restrictive legislation."); S. Rep. 99-541, at 3589 (1986) ("[T]he states must enact statutes which are *at least as restrictive* as the provisions of chapter 119 before they can authorize their state courts to issue interception orders."). "Rather than leaving no room for supplementary state regulation, Congress expressly authorized states to legislate in this field. Congress apparently wanted to ensure that states meet baseline standards, however, and thus federal law supersedes to the extent that state laws offer less protection than their federal counterparts." *Shively*, No. C-11-5775 EMC, 2012 WL 3026553 at *7. *Bunnell* and *Google Street View*, the two cases cited by Defendants, "are, by far, in the minority." *Leong*, No. 12-01562 GAF (MRWx), 2012 WL 1463313 at *3.

In addition, Defendants' misstate the nature of Plaintiffs' claims by arguing "each of plaintiffs' state-law claims is based on an alleged interception of electronic communications[.]" Mot. to Dismiss 24:9-10. As explained above, Plaintiffs would have a claim for damages even if the Defendants' scheme did not involve electronic communications. Moreover, to Plaintiffs' knowledge, no court has ever held that the federal Wiretap Act pre-empts traditional common law claims that pre-dated the Act's creation in 1968. *See In re: Google Street View*, 794 F. Supp. 2d 1067, 1085-86 (N.D. Cal. 2011) (Wiretap does not pre-empt non-CIPA cause-of-action).

Extra-territoriality – There's nothing extra-territorial about CIPA's application to this case. Facebook (1) is a California company that (2) directs its Internet tracking activities from California, (3) receives tracked Internet communications in California, (4) includes a binding Terms of Use adopting California law to govern all disputes with its members, and (5) upon information and belief, requires web-developers utilizing Facebook source code to also adopt California law. Compl. ¶ 306. Thus, a substantial portion of the challenged conduct (including that of the health care Defendants) occurred in California by virtue of Facebook's activities here and the health care Defendants have consented to the application of California law to govern its relationship with Facebook. *Id.* at ¶ 306e.

Moreover, CIPA's plain language applies to out-of-state wiretappers "who aid, agree[] with, employ[], or conspire[] with any person to … permit, or cause to be done any of the acts" prohibited by CIPA. Cal. Penal Code § 631(a). Those prohibited acts are as follows:

> Any person who … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, *or received at any place within this state*; or *who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained* ….

Plaintiffs have adequately alleged that Facebook received the information in California and that Facebook directs its tracking activities in California. Compl. ¶ 306b-c. CIPA applies.

4. Plaintiffs State Claims for California Constitutional Invasion of Privacy and Intrusion Upon Seclusion

Invasion of Privacy – As described by the California Supreme Court, the purpose of California's constitutional invasion of privacy tort "is readily discernible" as the initiatives text warned of "unnecessary information gathering by public and private entities – [such as] computer stored and generated dossiers and cradle-to-grave profiles on every American." *Hill v. NCAA*, 7 Cal. 4th 1, 15 (1994). "The evil addressed is … business conduct in collecting and stockpiling information … [and] [t]he Privacy Initiative's primary purpose is to afford some individuals some measure of protection against this most modern threat to personal privacy." *Id.* at 21. A California invasion of privacy claim is "not so much one of total secrecy as it is of the right to define one's

circle of intimacy – to choose who shall see beneath the quotidian mask." *Id.* at 25. Invasion of privacy has three elements: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Id.* at 39-40. Plaintiffs have adequately alleged all three elements.

Plaintiffs alleged "legally protected privacy interests" in the form of (a) the ECPA's Wiretap and Pen Register provisions;[25] (b) the Computer Fraud and Abuse Act and its state corollaries; (c) CIPA; (d) HIPAA; (e) Cal. Civ. Code § 1798.91; and (e) the privacy promises of the health care Defendants. Compl. ¶ 325. Plaintiffs alleged reasonable expectations of privacy[26] through these legally protected privacy interests and the health care Defendants' privacy promises. *See Riley*, 134 S. Ct. at 2473 (Data contained on smartphone, include visits to WebMD); *Norman-Bloodsaw*, 135 F.3d at 1260 (medical information); *In re: Nickelodeon*, 2016 WL 3513782 (violation of Internet privacy promises); *In re: Google Cookie Placement*, 806 F.3d at 150 (violation of Internet privacy promises); *Opperman*, 87 F. Supp. 3d 1018, 1059 (contact lists); *Lawlor v. North American Corp. of Ill.*, 983 N.E.2d 414, 426 (Ill. 2012) (phone records). Finally, Plaintiffs alleged serious invasions of privacy that constitute an egregious breach of social norms. *In re: Google Cookie Placement*, 806 F.3d at 150 (obtaining information through "deceit and disregard."); *In re: Nickelodeon*, 2016 WL 3513782 (3d Cir. June 27, 2016) (collecting information through dubious tactics); *Opperman* 87 F. Supp. 3d at 1061 ("Surreptitious theft of personal contact information … has [not] come to [be] qualified as 'routine commercial behavior.'"); *Campbell v. Facebook*, 77 F. Supp. 3d 836 (N.D. Cal. 2014) (analyzing Wiretap claim, "The court rejects the suggestion that any activity that generates revenue for a company should be considered within the 'ordinary course of business.'").

[25] The Pen Register Act prohibits non-consensual use of a "pen register" to track "dialing, routing, addressing, or signaling information" without consent. 18 U.S.C. § 3121, *et seq.* Thus, even if this Court finds that the URLs alleged do not contain content, Plaintiffs still have a legally protected privacy interest in DRAS.

[26] Through the Pen Register Act, plaintiffs distinguish between a reasonable expectation of privacy against disclosure of information to the government versus a reasonable expectation against disclosure to a private entity. Under the Pen Register Act, American consumers have a reasonable expectation of privacy that a private party cannot install a pen register or trap and trace device without their consent or an exception authorized by the Act. 18 U.S.C. § 3121, *et seq.* As detailed herein, Defendant Facebook has publicly referred to warrantless collection of mere IP addresses by government agents as raising "civil liberties and human rights concerns."

Intrusion Upon Seclusion – "Intrusion upon seclusion" is similar but distinct from invasion of privacy. To make a claim for intrusion, a plaintiff must allege an intrusion into a private matter, including "some zone of … privacy surrounding, or obtain[ing] unwanted access to data about the plaintiff … [and] an objectively reasonable expectation" of privacy in "the place, conversation, or data source." *Shulman v. Group W. Prods., Inc*., 18 Cal. 4th 200, 232 (1998). In this case, Plaintiffs allege objectively reasonable expectations of privacy based upon federal and state statutes as well as the explicit promises made by the health care Defendants with which they were communicating.

Second, the plaintiff must allege that the intrusion is "highly offensive" to a reasonable person. For both intrusion and invasion of privacy, "highly offensive" or "serious" is ultimately a jury question, but first a court must determine "whether, as a matter of policy, such conduct should be considered, as a matter of law, not highly offensive." *Taus v. Loftus*, 40 Cal. 4th 683, 737 (2007). Congress and every state has already made this "policy" decision through the passage of criminal and civil laws designed to protect communications and health care privacy. Violation of the ECPA or CFAA subjects a defendant to imprisonment. Violation of HIPAA subjects covered entities to substantial fines and other civil penalties. Beyond criminal penalties, California explicitly declared that the activities in this case are a "serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630. Further, the California Supreme Court explicitly held that "eavesdropping [or] wiretapping" gives rise to the tort of intrusion upon seclusion. *Shulman* at 863, 868. Because this case involves the unauthorized tracking and disclosure of sensitive medical information protected by the Constitution, common law, statutes, and regulations, a reasonable jury could find the intrusions "highly offensive" or "serious."

5. The Claim for Negligence Per Se Is Valid

A presumption of negligence is created when four elements are established: (1) [the defendant] violated a statute, ordinance, or regulation of a public entity; (2) the violation proximately caused death or injury to person or property; (3) the injury resulted from an occurrence of the nature which the statute, ordinance, or regulation was designed to prevent; and (4) the person suffering the injury to his person or property was one of the class of persons for whose protection the statute, ordinance, or regulation was adopted. Cal. Evid. Code § 669(a); *Quiroz v. Seventh Ave.*

Ctr., 140 Cal. App. 4th 1256, 1285 (2006) (citing same).

Plaintiffs allege that Defendants' conduct violated HIPAA, which is a statute of a public entity, and that the violation proximately caused them injury. HIPAA was enacted to prevent unauthorized use of personally identifiable health information, and protects individuals to whom health information relates. To de-identify health information, HIPAA requires removal of the names "of the individual or of the relatives, employers, or household members of the individual." 45 C.F.R. § 164.514(b)(2)(i)(A). IP addresses must also be removed. 45 C.F.R. § 164.514(b)(2)(i)(O). As alleged, the information transmitted to Facebook, which contained health information, was not de-identified. As individuals seeking information about their own health conditions or those of a household member, each Plaintiff falls into the class of persons HIPAA aims to protect.

Defendants' violation of the statute proximately caused Plaintiffs injury – namely, the violation of their rights to privacy in their health information. The violation of this right is precisely the type of occurrence that HIPAA was enacted to prevent. Therefore, Plaintiffs have alleged all elements of a negligence claim under a negligence per se theory.

While there is an economic component to the injury alleged by Plaintiffs (namely, the value of their data), the loss that Plaintiffs allege is not strictly economic. HIPAA conferred upon the health care Defendants that are covered entities a duty to keep Plaintiffs' health information private. As a result of the health care Defendants' breach of this duty, Plaintiffs' privacy rights were violated causing them harm and Defendants liable for that damage.

6. <u>The Claim For Negligent Disclosure of Confidential Information Is Valid</u>

Even non-health care websites have a legal obligation to keep the privacy promises they make. *See In re: Nickelodeon,* 2016 WL 3513782 ("Viacom created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses."). In this case, the health care Defendants explicitly promised not to disclose the plaintiffs' PII and communications to third-parties, with limited exceptions that do not apply here. And then they did so anyway. Like Viacom, they helped create the expectation and a duty to keep their promise, then they breached it.

Defendants' argument about referer headers and public URLs obfuscates the facts of this case. As discussed at length above, and set forth in the Complaint, the disclosures also included PII connected to sensitive health communications. Defendants argue that because public URLs are not protected health information, HIPAA's restrictions are irrelevant. Again, Defendants distort the facts. Plaintiffs have not alleged that use of anonymous URLs violates HIPAA. Instead, this case is about sensitive communications attached to PII. In these exchanges, Facebook acquires not only information sufficient to identify the visitor, but also content pertinent to his or her health condition. As discussed above, the Ninth Circuit has held that URLs contain "content" when they include search terms or similar communications made by the user. *In re: Zynga*, 750 F.3d at 1109. For example, the text following ".org" in the URL that Plaintiff Jane Doe II visited, http://my.clevelandclinig.org/search/results?q=intestine%20transplant (Compl. ¶ 188), would constitute "content."

As is required to assert a negligence claim under California law, Plaintiffs alleged "appreciable, nonspeculative, present harm." *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962 (S.D. Cal. 2012) (citing *Aas v. Superior Court*, 24 Cal. 4th 627, 646 (2000)); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009), aff'd, 380 Fed.Appx. 689 (9th Cir. 2010)). This harm need not be tangible. Plaintiffs were personally harmed when their sensitive medical information was disclosed to, tracked, and intercepted by Facebook without their knowledge or consent, rendering their information no longer private. To call into question whether such an invasion of Plaintiffs' privacy constitutes sufficient harm is to question whether the privacy of one's health information has value at all. If health information were worthless, statutes such as HIPAA would serve no purpose. The very existence of numerous federal and state laws protecting individuals' privacy demonstrates widespread recognition that privacy, particularly of sensitive medical information, is inherently valuable. Because the right to privacy in certain information is intrinsically valuable, the loss of such privacy through improper disclosure causes actual harm.

Further, Plaintiffs' allegations of actual harm distinguish their case from *In re Sony* and *Regents of Univ. of Cal. v. Superior Court*, where the plaintiffs did not allege that the data at issue

had been misused. 903 F. Supp. 2d at 962-63 (dismissing negligence claim where plaintiffs alleged exposure to increased identity theft and fraud risks); 220 Cal. App. 4th 549 (2013) (dismissing claim for negligent disclosure of information where plaintiffs could not allege misuse of same).

7. The Claim for Breach of Fiduciary Duty of Confidentiality Survives

Establishing the tort for violation of a fiduciary duty requires: (1) a breach; (2) of a fiduciary duty; and (3) that the plaintiff suffered damages proximately caused by defendant's conduct. Restatement (Second) of Torts, § 874 (1979). The comment to Restatement (Second) of Torts § 874 explains:

> *A fiduciary relation exists between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation* . . . the beneficiary is entitled to tort damages for harm caused by the breach of duty arising from the relation. … In addition to or in substitution for these damages the beneficiary may be entitled to restitutionary recovery, since not only is he entitled to recover for any harm done to his legally protected interests by the wrongful conduct of the fiduciary, but ordinarily he is entitled to profits that result to the fiduciary from his breach of duty and to be the beneficiary of a constructive trust in the profits. . . . A person who knowingly assists a fiduciary in committing a breach of trust is himself guilty of tortious conduct and is subject to liability for the harm thereby caused.

Restatement (Second) of Torts § 874, cmts. (a)-(c) (emphasis added). One breach of fiduciary duty commonly regarded as giving rise to an action in tort is the disclosure of confidential information. *See, e.g., Horne v. Patton*, 287 So. 2d 824 (Ala. 1973); *Cannell v. Medical & Surgical Clinic*, 315 N.E.2d 278 (Ill. App. Ct. 1974); *Felis v. Greenberg*, 273 N.Y.S.2d 288 (N.Y. Sup. Ct. 1966); *Doe v. Roe*, 400 N.Y.S.2d 668 (N.Y. Sup. Ct. 1977); *Schaffer v. Spicer*, 215 N.W.2d 134 (S.D. 1974). The Northern District of California has opined on the importance of a "confidential relationship" in the context of a fiduciary duty:

> A "confidential relationship" arises only "where a confidence is reposed by one person in the integrity of another, and . . . the party in whom the confidence is reposed . . . voluntarily accepts or assumes to accept the confidence." Significantly, in the context of claims for breach of fiduciary duty . . . '[t]he essence of a fiduciary or confidential relationship is that the parties do not deal on equal terms, because the person in whom trust and confidence is reposed and who accepts that trust and confidence is in a superior position to exert unique influence over the dependent party.

City Sols., Inc. v. Clear Channel Commc'ns, Inc., 201 F. Supp. 2d 1048, 1050-51 (N.D. Cal. 2002) (citing *Barbara A. v. John G.*, 145 Cal. App. 3d 369, 382–83 (1983); *Vai v. Bank of America*, 56

Cal. 2d 329, 338 (1961) ("The key factor in the existence of a fiduciary relationship lies in control by a person over the property of another")).

Here, Plaintiffs placed their confidence in Defendants that Plaintiffs' confidential medical data and communications with Defendants' websites regarding their medical conditions would be kept private. Defendants' complete control over Plaintiffs' information, as alleged in the Complaint, demonstrates a relationship that is not on equal footing. Despite this inequality, which strongly suggests a confidential relationship that creates a duty, Defendants argue that their privacy policies do not guarantee any privacy of Plaintiffs' information. But, the very titles of these "privacy policies" belie Defendants' argument, as they would have this Court believe that what they actually have are not "privacy policies" but "lack of privacy policies." Regardless of Defendants' assertions to the contrary, the privacy policies and confidential relationships between the parties create a duty.

Defendants do not challenge the breach requirement in section 874, so there is no need to address this point. Finally, as to damages, the comment to section 874 quoted *supra* provides a clear measure for damages. *See* Restatement (Second) of Torts, §§ 874, 875 ("Each of two or more persons whose tortious conduct is a legal cause of a single and indivisible harm to the injured party is subject to liability to the injured party for the entire harm."), 876 ("[H]arm resulting to a third person from the tortious conduct of another, one is subject to liability . . . ."); *see also*, Restatement (Second) of Torts § 874, cmt. (c) (liability for breach of fiduciary duty applies to both breaching party and any other party acting in concert). Accordingly, this claim should proceed.

Finally, amongst other damages, Plaintiffs are "entitled to profits that result to the fiduciary from his breach of duty." Even if the health care Defendants do not directly profit from pilfering Plaintiffs' information and selling it to Facebook (not alleged in the Complaint), all Defendants are still liable to Plaintiffs because Facebook profited from the information, as collecting/selling personal information is an inherent part of its business model, as set out above.

8. <u>The Breach of Duty of Good Faith and Fair Dealing Is Proper</u>

Plaintiffs' have adequately stated a Good Faith and Fair Dealing claim against Facebook. Citing only *Partti v. Palo Alto Med. Found. for Health Care, Research & Educ., Inc.*, 2015 WL 6664477 (N.D. Cal. Nov. 2, 2015), Facebook ignores the full quote therefrom, choosing instead

selective words from the holding. Mot. to Dismiss 32:23-25. The full quote reads: "If the allegations do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action**,** they may be disregarded as superfluous as no additional claim is actually stated." (citing *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1394, as modified on denial of reh'g (2001)). Here Plaintiffs allege a breach and seek relief different and independent from relief claimed under other counts. Furthermore, there is no companion contract cause of action in the Complaint. In the Order Granting Summary Judgment in *Partti*, Judge Grewal held, "In order for Defendants to have breached the implied covenant, there must be a contract to breach." *Partti* at 10. Here, there is a contract, an implied duty, and a breach.

9. The Fraud Claim Is Proper

To state an action for fraud, a plaintiff must plead with specificity an intentional misrepresentation of material fact with knowledge of its falsity and intent to induce reliance, actual reliance, and damages proximately caused by the reliance. *Gonsalves v. Hodgson*, 38 Cal. 2d 91, 100-02 (1951). Plaintiffs' actual and constructive fraud claims satisfy Rule 9(b)'s specificity requirement. Plaintiffs allege the "who" (Facebook and its employees, along with the health care Defendants), the "what" (surreptitious tracking and interception of private health-related communications), the "when" (during the class period), the "where" (in the interactions between Plaintiffs' computers, health care Defendants' websites, and Facebook's servers) and the "how" (through specifically identified, improperly planted cookies that track and intercept communications). Having falsely promised that they would only share health-related information in limited circumstances, the Defendants were duty-bound to protect this information from improper tracking and interception.

Defendants argue that Facebook made no misrepresentation – essentially, that Plaintiffs were aware of and consented to the improper tracking and interception. This argument is without merit, as discussed above. Plaintiffs alleged intent to deceive, reliance, and damages arising therefrom, which satisfies the elements set forth in *Gonsalves*. 38 Cal. 2d 91.

10. The Quantum Meruit Claims Were Properly Alleged

The Complaint includes sufficient allegations to support a claim of quantum meruit. "The underlying idea behind quantum meruit is the law's distaste for unjust enrichment. If one has received a benefit which one may not justly retain, one should 'restore the aggrieved party to his [or her] former position by return of the thing *or its equivalent* in money." *Maglica v. Maglica*, 66 Cal. App. 4th 442, 449 (1992) (emphasis added) (internal citations omitted). Should Plaintiffs be unable to prove a binding contract between Facebook and them, or elect to rescind it, they are not without remedy. Plaintiffs' sensitive medical information was collected for the purpose of direct marketing. Compl. ¶ 370. Facebook cannot justly retain the benefit it obtained (Compl. ¶ 80) from violating Plaintiffs' privacy rights (Compl. ¶ 371). Plaintiffs would therefore be entitled to compensation for the value of their personally identifiable health-related information pursuant to quantum meruit.

V. CONCLUSION

For the foregoing facts and reasons, the Motion should be denied in its entirety and Defendants ordered to Answer. If the Motion is granted, either in whole or in part, Plaintiffs hereby request leave to amend.

DATED: August 1, 2016

KIESEL LAW LLP

By: */s/ Jeffrey A. Koncius*
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

THE GORNY LAW FIRM, LC
Stephen M. Gorny [Admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [Admitted *Pro Hac Vice*]
chris@gornylawfirm.com
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

BARNES & ASSOCIATES

Jay Barnes [Admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [Admitted *Pro Hac Vice*]
rod.chapel@gmail.com
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

EICHEN CRUTCHLOW ZASLOW & McELROY

Barry. R. Eichen [Admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [Admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
Ashley A. Smith [Admitted *Pro Hac Vice*]
asmith@njadvocates.com
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

THE SIMON LAW FIRM, P.C.

Amy Gunn [Admitted *Pro Hac Vice*]
agunn@simonlawpc.com
800 Market St., Ste. 1700
St. Louis, MO 63101
Tel.: 314-241-2929
Fax: 314-241-2029

BERGMANIS LAW FIRM, L.L.C.

Andrew Lyskowski [to be admitted *Pro Hac Vice*]
alyskowski@ozarklawcenter.com
380 W. Hwy. 54, Ste. 201
Camdenton, MO 65020
Tel.: 573-346-2111
Fax: 573-346-5885